Bulletin (SB17-149)

Vulnerability Summary for the Week of May 22, 2017

Original release date: May 29, 2017

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "Kernel" component. A race condition allows attackers to execute arbitrary code in a privileged context via a crafted app.	2017-05-22	7.6	CVE-2017-2501 BID CONFIRM CONFIRM CONFIRM CONFIRM
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "SQLite" component. A use-after-free vulnerability allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted SQL statement.	2017-05-22	7.5	CVE-2017-2513 BID CONFIRM CONFIRM CONFIRM CONFIRM
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-05-22	9.3	CVE-2017-2494 CONFIRM
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "Intel Graphics Driver" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-05-22	9.3	CVE-2017-2503 CONFIRM
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer overflow in the pnm_load_ascii function in input-pnm.c:303:12.	2017-05-23	7.5	CVE-2017-9151 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer over-read in the pnm_load_raw function in input-pnm.c:346:41.	2017-05-23	7.5	CVE-2017-9152 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer overflow in the pnm_load_rawpbm function in input-pnm.c:391:13.	2017-05-23	7.5	CVE-2017-9153 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a stack-based buffer overflow in the pnmscanner_gettoken function in input-pnm.c:458:12.	2017-05-23	7.5	CVE-2017-9160 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a "cannot be represented in type int" issue in autotrace.c:188:23.	2017-05-23	7.5	CVE-2017-9161 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a "cannot be represented in type int" issue in autotrace.c:191:2.	2017-05-23	7.5	CVE-2017-9162 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a "cannot be represented in type int" issue in pxl-outline.c:106:54.	2017-05-23	7.5	CVE-2017-9163 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer over-read in the GET_COLOR function in color.c:16:11.	2017-05-23	7.5	CVE-2017-9164 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer over-read in the GET_COLOR function in color.c:17:11.	2017-05-23	7.5	CVE-2017-9165 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer over-read in the GET_COLOR function in color.c:18:11.	2017-05-23	7.5	CVE-2017-9166 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer overflow in the ReadImage function in input-bmp.c:337:25.	2017-05-23	7.5	CVE-2017-9167 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer overflow in the ReadImage function in input-bmp.c:353:25.	2017-05-23	7.5	CVE-2017-9168 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer overflow in the ReadImage function in input-bmp.c:355:25.	2017-05-23	7.5	CVE-2017-9169 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer overflow in the ReadImage function in input-bmp.c:370:25.	2017-05-23	7.5	CVE-2017-9170 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer over-read in the ReadImage function in input-bmp.c:492:24.	2017-05-23	7.5	CVE-2017-9171 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer overflow in the ReadImage function in input-bmp.c:496:29.	2017-05-23	7.5	CVE-2017-9172 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer overflow in the ReadImage function in input-bmp.c:497:29.	2017-05-23	7.5	CVE-2017-9173 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a "cannot be represented in type int" issue in input-bmp.c:309:7.	2017-05-23	7.5	CVE-2017-9183 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a "cannot be represented in type int" issue in input-bmp.c:314:7.	2017-05-23	7.5	CVE-2017-9184 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a "cannot be represented in type int" issue in input-bmp.c:319:7.	2017-05-23	7.5	CVE-2017-9185 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a "cannot be represented in type int" issue in input-bmp.c:326:17.	2017-05-23	7.5	CVE-2017-9186 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a "cannot be represented in type int" issue in input-bmp.c:486:7.	2017-05-23	7.5	CVE-2017-9187 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a "left shift ... cannot be represented in type int" issue in input-bmp.c:516:63.	2017-05-23	7.5	CVE-2017-9188 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer overflow in the rle_fread function in input-tga.c:252:15.	2017-05-23	7.5	CVE-2017-9191 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer overflow in the ReadImage function in input-tga.c:528:7.	2017-05-23	7.5	CVE-2017-9192 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer over-read in the ReadImage function in input-tga.c:538:33.	2017-05-23	7.5	CVE-2017-9193 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer over-read in the ReadImage function in input-tga.c:559:29.	2017-05-23	7.5	CVE-2017-9194 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a heap-based buffer over-read in the ReadImage function in input-tga.c:620:27.	2017-05-23	7.5	CVE-2017-9195 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a "negative-size-param" issue in the ReadImage function in input-tga.c:528:7.	2017-05-23	7.5	CVE-2017-9196 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a "cannot be represented in type int" issue in input-tga.c:498:55.	2017-05-23	7.5	CVE-2017-9197 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a "cannot be represented in type int" issue in input-tga.c:508:18.	2017-05-23	7.5	CVE-2017-9198 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a "cannot be represented in type int" issue in input-tga.c:192:19.	2017-05-23	7.5	CVE-2017-9199 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 has a "cannot be represented in type int" issue in input-tga.c:528:63.	2017-05-23	7.5	CVE-2017-9200 MISC
cisco -- firepower_threat_defense	A vulnerability in the logging configuration of Secure Sockets Layer (SSL) policies for Cisco FirePOWER System Software 5.3.0 through 6.2.2 could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition due to high consumption of system resources. The vulnerability is due to the logging of certain TCP packets by the affected software. An attacker could exploit this vulnerability by sending a flood of crafted TCP packets to an affected device. A successful exploit could allow the attacker to cause a DoS condition. The success of an exploit is dependent on how an administrator has configured logging for SSL policies for a device. This vulnerability affects Cisco FirePOWER System Software that is configured to log connections by using SSL policy default actions. Cisco Bug IDs: CSCvd07072.	2017-05-21	7.8	CVE-2017-6632 BID CONFIRM
dropbear_ssh_project -- dropbear_ssh	The server in Dropbear before 2017.75 might allow post-authentication root remote code execution because of a double free in cleanup of TCP listeners when the -a option is enabled.	2017-05-19	9.3	CVE-2017-9078 CONFIRM
libtiff -- libtiff	In LibTIFF 4.0.7, the program processes BMP images without verifying that biWidth and biHeight in the bitmap-information header match the actual input, leading to a heap-based buffer over-read in bmp2tiff.	2017-05-21	7.5	CVE-2017-9117 MISC BID
mimosa -- client_radios	An issue was discovered on Mimosa Client Radios before 2.2.3 and Mimosa Backhaul Radios before 2.2.3. In the device's web interface, after logging in, there is a page that allows you to ping other hosts from the device and view the results. The user is allowed to specify which host to ping, but this variable is not sanitized server-side, which allows an attacker to pass a specially crafted string to execute shell commands as the root user.	2017-05-21	9.0	CVE-2017-9133 MISC
mimosa -- client_radios	An issue was discovered on Mimosa Client Radios before 2.2.4 and Mimosa Backhaul Radios before 2.2.4. On the backend of the device's web interface, there are some diagnostic tests available that are not displayed on the webpage; these are only accessible by crafting a POST request with a program like cURL. There is one test accessible via cURL that does not properly sanitize user input, allowing an attacker to execute shell commands as the root user.	2017-05-21	9.0	CVE-2017-9135 MISC
mimosa -- client_radios	An issue was discovered on Mimosa Client Radios before 2.2.3. In the device's web interface, there is a page that allows an attacker to use an unsanitized GET parameter to download files from the device as the root user. The attacker can download any file from the device's filesystem. This can be used to view unsalted, MD5-hashed administrator passwords, which can then be cracked, giving the attacker full admin access to the device's web interface. This vulnerability can also be used to view the plaintext pre-shared key (PSK) for encrypted wireless connections, or to view the device's serial number (which allows an attacker to factory reset the device).	2017-05-21	7.8	CVE-2017-9136 MISC

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
allendisk_project -- allendisk	reg.php in Allen Disk 1.6 doesn't check if isset($_SESSION['captcha']['code'])==1, which makes it possible to bypass the CAPTCHA via an empty $_POST['captcha'].	2017-05-19	5.0	CVE-2017-9090 CONFIRM
allendisk_project -- allendisk	/admin/loginc.php in Allen Disk 1.6 doesn't check if isset($_SESSION['captcha']['code']) == 1, which leads to CAPTCHA bypass by emptying $_POST['captcha'].	2017-05-19	5.0	CVE-2017-9091 CONFIRM
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. The issue involves the "Safari" component. It allows remote attackers to cause a denial of service (application crash) via a crafted web site that improperly interacts with the history menu.	2017-05-22	4.3	CVE-2017-2495 CONFIRM CONFIRM
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-05-22	6.8	CVE-2017-2496 CONFIRM CONFIRM
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. The issue involves the "iBooks" component. It allows remote attackers to trigger visits to arbitrary URLs via a crafted book.	2017-05-22	5.8	CVE-2017-2497 CONFIRM CONFIRM
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. The issue involves the "Security" component. It allows attackers to bypass intended access restrictions via an untrusted certificate.	2017-05-22	5.0	CVE-2017-2498 BID CONFIRM
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. tvOS before 10.2.1 is affected. The issue involves the "WebKit Web Inspector" component. It allows attackers to execute arbitrary unsigned code or cause a denial of service (memory corruption) via a crafted app.	2017-05-22	6.8	CVE-2017-2499 CONFIRM CONFIRM CONFIRM
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "CoreAudio" component. It allows attackers to bypass intended memory-read restrictions via a crafted app.	2017-05-22	4.3	CVE-2017-2502 BID CONFIRM CONFIRM CONFIRM CONFIRM
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. tvOS before 10.2.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to conduct Universal XSS (UXSS) attacks via a crafted web site that improperly interacts with WebKit Editor commands.	2017-05-22	4.3	CVE-2017-2504 CONFIRM CONFIRM CONFIRM
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. tvOS before 10.2.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-05-22	6.8	CVE-2017-2505 CONFIRM CONFIRM CONFIRM
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-05-22	6.8	CVE-2017-2506 CONFIRM CONFIRM
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-05-22	6.8	CVE-2017-2514 CONFIRM CONFIRM
apple -- iphone_os	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. tvOS before 10.2.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-05-22	6.8	CVE-2017-2515 CONFIRM CONFIRM CONFIRM
apple -- safari	An issue was discovered in certain Apple products. Safari before 10.1.1 is affected. The issue involves the "Safari" component. It allows remote attackers to spoof the address bar via a crafted web site.	2017-05-22	4.3	CVE-2017-2500 CONFIRM
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid read and SEGV), related to the GET_COLOR function in color.c:16:11.	2017-05-23	5.0	CVE-2017-9154 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid read and SEGV), related to the input_pnm_reader function in input-pnm.c:243:3.	2017-05-23	5.0	CVE-2017-9155 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid write and SEGV), related to the pnm_load_ascii function in input-pnm.c:303:12.	2017-05-23	5.0	CVE-2017-9156 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid write and SEGV), related to the pnm_load_ascii function in input-pnm.c:306:14.	2017-05-23	5.0	CVE-2017-9157 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid write and SEGV), related to the pnm_load_raw function in input-pnm.c:336:11.	2017-05-23	5.0	CVE-2017-9158 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid write and SEGV), related to the pnm_load_rawpbm function in input-pnm.c:391:15.	2017-05-23	5.0	CVE-2017-9159 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid read and SEGV), related to the GET_COLOR function in color.c:21:23.	2017-05-23	5.0	CVE-2017-9174 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid write and SEGV), related to the ReadImage function in input-bmp.c:353:25.	2017-05-23	5.0	CVE-2017-9175 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid write and SEGV), related to the ReadImage function in input-bmp.c:370:25.	2017-05-23	5.0	CVE-2017-9176 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid read and SEGV), related to the ReadImage function in input-bmp.c:390:12.	2017-05-23	5.0	CVE-2017-9177 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid write and SEGV), related to the ReadImage function in input-bmp.c:421:11.	2017-05-23	5.0	CVE-2017-9178 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid read and SEGV), related to the ReadImage function in input-bmp.c:425:14.	2017-05-23	5.0	CVE-2017-9179 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid read and SEGV), related to the ReadImage function in input-bmp.c:440:14.	2017-05-23	5.0	CVE-2017-9180 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid write and SEGV), related to the ReadImage function in input-bmp.c.	2017-05-23	5.0	CVE-2017-9181 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (use-after-free and invalid heap read), related to the GET_COLOR function in color.c:16:11.	2017-05-23	5.0	CVE-2017-9182 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid read and application crash), related to the GET_COLOR function in color.c:16:11.	2017-05-23	5.0	CVE-2017-9189 MISC
autotrace_project -- autotrace	libautotrace.a in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (invalid free), related to the free_bitmap function in bitmap.c:24:5.	2017-05-23	5.0	CVE-2017-9190 MISC
dropbear_ssh_project -- dropbear_ssh	Dropbear before 2017.75 might allow local users to read certain files as root, if the file has the authorized_keys file format with a command= option. This occurs because ~/.ssh/authorized_keys is read with root privileges and symlinks are followed.	2017-05-19	4.7	CVE-2017-9079 CONFIRM
google -- android	Integer overflow in soundtrigger/ISoundTriggerHwService.cpp in Android allows attacks to cause a denial of service via unspecified vectors.	2017-05-23	5.0	CVE-2015-1529 BID CONFIRM MISC
imagemagick -- imagemagick	In ImageMagick 7.0.5-7 Q16, a crafted file could trigger an assertion failure in the ResetImageProfileIterator function in MagickCore/profile.c because of missing checks in the ReadDDSImage function in coders/dds.c.	2017-05-22	4.3	CVE-2017-9141 BID CONFIRM CONFIRM
imagemagick -- imagemagick	In ImageMagick 7.0.5-7 Q16, a crafted file could trigger an assertion failure in the WriteBlob function in MagickCore/blob.c because of missing checks in the ReadOneJNGImage function in coders/png.c.	2017-05-22	4.3	CVE-2017-9142 CONFIRM CONFIRM
imagemagick -- imagemagick	In ImageMagick 7.0.5-5, the ReadARTImage function in coders/art.c allows attackers to cause a denial of service (memory leak) via a crafted .art file.	2017-05-22	4.3	CVE-2017-9143 CONFIRM CONFIRM
imagemagick -- imagemagick	In ImageMagick 7.0.5-5, a crafted RLE image can trigger a crash because of incorrect EOF handling in coders/rle.c.	2017-05-22	4.3	CVE-2017-9144 BID CONFIRM
imageworsener_project -- imageworsener	The my_skip_input_data_fn function in imagew-jpeg.c in libimageworsener.a in ImageWorsener 1.3.1 allows remote attackers to cause a denial of service (infinite loop) via a crafted image.	2017-05-19	4.3	CVE-2017-9093 CONFIRM
imageworsener_project -- imageworsener	The lzw_add_to_dict function in imagew-gif.c in libimageworsener.a in ImageWorsener 1.3.1 allows remote attackers to cause a denial of service (infinite loop) via a crafted image.	2017-05-19	4.3	CVE-2017-9094 CONFIRM
libtiff -- libtiff	LibTIFF 4.0.7 has an invalid read in the _TIFFVGetField function in tif_dir.c, which might allow remote attackers to cause a denial of service (crash) via a crafted TIFF file.	2017-05-22	4.3	CVE-2017-9147 MISC BID
mimosa -- client_radios	An issue was discovered on Mimosa Client Radios before 2.2.3 and Mimosa Backhaul Radios before 2.2.3. By connecting to the Mosquitto broker on an access point and one of its clients, an attacker can gather enough information to craft a command that reboots the client remotely when sent to the client's Mosquitto broker, aka "unauthenticated remote command execution." This command can be re-sent endlessly to act as a DoS attack on the client.	2017-05-21	5.0	CVE-2017-9131 MISC
mimosa -- client_radios	A hard-coded credentials issue was discovered on Mimosa Client Radios before 2.2.3, Mimosa Backhaul Radios before 2.2.3, and Mimosa Access Points before 2.2.3. These devices run Mosquitto, a lightweight message broker, to send information between devices. By using the vendor's hard-coded credentials to connect to the broker on any device (whether it be an AP, Client, or Backhaul model), an attacker can view all the messages being sent between the devices. If an attacker connects to an AP, the AP will leak information about any clients connected to it, including the serial numbers, which can be used to remotely factory reset the clients via a page in their web interface.	2017-05-21	5.0	CVE-2017-9132 MISC
mimosa -- client_radios	An information-leakage issue was discovered on Mimosa Client Radios before 2.2.3 and Mimosa Backhaul Radios before 2.2.3. There is a page in the web interface that will show you the device's serial number, regardless of whether or not you have logged in. This information-leakage issue is relevant because there is another page (accessible without any authentication) that allows you to remotely factory reset the device simply by entering the serial number.	2017-05-21	5.0	CVE-2017-9134 MISC

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- linux_kernel	The do_check function in kernel/bpf/verifier.c in the Linux kernel before 4.11.1 does not make the allow_ptr_leaks value available for restricting the output of the print_bpf_insn function, which allows local users to obtain sensitive address information via crafted bpf system calls.	2017-05-22	2.1	CVE-2017-9150 MISC MISC MISC MISC
rsa -- adaptive_authentication_(on_premise)	EMC RSA Adaptive Authentication (On-Premise) versions prior to 7.3 P2 (exclusive) contains a fix for a cross-site scripting vulnerability that could potentially be exploited by malicious users to compromise the affected system.	2017-05-19	3.5	CVE-2017-4978 CONFIRM BID

Back to top

Severity Not Yet Assigned			
Primary Vendor -- Product	Description	Published	CVSS Sco
7_zip -- 7_zip_for_windows	Untrusted search path vulnerability in 7 Zip for Windows 16.02 and earlier allows remote attackers to gain privileges via a Trojan horse DLL in an unspecified directory.	2017-05-22	not calcu
alienvault -- ossim	The sudoers file in the asset discovery scanner in AlienVault OSSIM before 5.0.1 allows local users to gain privileges via a crafted nmap script.	2017-05-23	not calcu
alienvault -- ossim	The asset discovery scanner in AlienVault OSSIM before 5.0.1 allows remote authenticated users to execute arbitrary commands via the assets array parameter to netscan/do_scan.php.	2017-05-23	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
apache--archiva	Several REST service endpoints of Apache Archiva are not protected against Cross Site Request Forgery (CSRF) attacks. A malicious site opened in the same browser as the archiva site, may send an HTML response that performs arbitrary actions on archiva services, with the same rights as the active archiva session (e.g. administrator rights).	2017-05-22	not calcu
apache--knox	For versions of Apache Knox from 0.2.0 to 0.11.0 - an authenticated user may use a specially crafted URL to impersonate another user while accessing WebHDFS through Apache Knox. This may result in escalated privileges and unauthorized data access. While this activity is audit logged and can be easily associated with the authenticated user, this is still a serious security issue. All users are recommended to upgrade to the Apache Knox 0.12.0 release.	2017-05-26	not calcu
apple--ios_macos	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. The issue involves the "SQLite" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-05-22	not calcu
apple--ios_safari	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to conduct Universal XSS (UXSS) attacks via a crafted web site that improperly interacts with cached frames.	2017-05-22	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
apple_ios_safari	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-05-22	not calcu
apple_ios_safari	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to conduct Universal XSS (UXSS) attacks via a crafted web site that improperly interacts with container nodes.	2017-05-22	not calcu
apple_ios_safari	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to conduct Universal XSS (UXSS) attacks via a crafted web site that improperly interacts with pageshow events.	2017-05-22	not calcu
apple_ios_safari	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-05-22	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
apple_ios_safari	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-05-22	not calcu
apple_ios_safari	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-05-22	not calcu
apple_ios	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. The issue involves the "Notifications" component. It allows attackers to cause a denial of service via a crafted app.	2017-05-22	not calcu
apple_macos	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "WindowServer" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-05-22	not calcu
apple_macos	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "802.1X" component. It allows remote attackers to discover the network credentials of arbitrary users by operating a crafted network that requires 802.1X authentication, because EAP-TLS certificate validation mishandles certificate changes.	2017-05-22	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
apple -- macos	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "HFS" component. It allows attackers to bypass intended memory-read restrictions via a crafted app.	2017-05-22	not calcu
apple -- macos	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "iBooks" component. It allows attackers to conduct sandbox-escape attacks or cause a denial of service (memory corruption) via a crafted app.	2017-05-22	not calcu
apple -- macos	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "NVIDIA Graphics Drivers" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-05-22	not calcu
apple -- macos	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "Accessibility Framework" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-05-22	not calcu
apple -- macos	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-05-22	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
apple -- macos	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "IOGraphics" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-05-22	not calcu
apple -- macos	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "WindowServer" component. It allows attackers to bypass intended memory-read restrictions via a crafted app.	2017-05-22	not calcu
apple -- macos	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "Speech Framework" component. It allows attackers to conduct sandbox-escape attacks or cause a denial of service (memory corruption) via a crafted app.	2017-05-22	not calcu
apple -- macos	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-05-22	not calcu
apple -- macos	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "Multi-Touch" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-05-22	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
apple -- macos	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "Multi-Touch" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-05-22	not calcu
apple -- macos	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "Sandbox" component. It allows attackers to conduct sandbox-escape attacks or cause a denial of service (memory corruption) via a crafted app.	2017-05-22	not calcu
apple -- macos	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "Security" component. It allows attackers to conduct sandbox-escape attacks or cause a denial of service (resource consumption) via a crafted app.	2017-05-22	not calcu
apple -- macos	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "Kernel" component. It allows attackers to bypass intended memory-read restrictions via a crafted app.	2017-05-22	not calcu
apple -- macos	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "Speech Framework" component. It allows attackers to conduct sandbox-escape attacks via a crafted app.	2017-05-22	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
apple -- macos	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "WindowServer" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-05-22	not calcu
apple -- macos	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "WindowServer" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-05-22	not calcu
apple -- macos	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "DiskArbitration" component. A race condition allows attackers to execute arbitrary code in a privileged context via a crafted app.	2017-05-22	not calcu
apple -- macos	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "CoreAnimation" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory consumption and application crash) via crafted data.	2017-05-22	not calcu
apple -- macos	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue involves the "Kernel" component. It allows attackers to bypass intended memory-read restrictions via a crafted app.	2017-05-22	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
apple_multiple_products	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "SQLite" component. It allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a crafted SQL statement.	2017-05-22	not calcu
apple_multiple_products	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "CoreFoundation" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via crafted data.	2017-05-22	not calcu
apple_multiple_products	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "Kernel" component. It allows attackers to bypass intended memory-read restrictions via a crafted app.	2017-05-22	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
apple_multiple_products	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "Foundation" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via crafted data.	2017-05-22	not calcu
apple_multiple_products	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. tvOS before 10.2.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-05-22	not calcu
apple_multiple_products	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. tvOS before 10.2.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-05-22	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
apple_multiple_products	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. iTunes before 12.6.1 on Windows is affected. tvOS before 10.2.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-05-22	not calcu
apple_multiple_products	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "TextInput" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via crafted data.	2017-05-22	not calcu
apple_multiple_products	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. tvOS before 10.2.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to conduct Universal XSS (UXSS) attacks via a crafted web site that improperly interacts with frame loading.	2017-05-22	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
apple -- multiple_products	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "Kernel" component. It allows attackers to bypass intended memory-read restrictions via a crafted app.	2017-05-22	not calcu
apple -- multiple_products	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "AVEVideoEncoder" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-05-22	not calcu
apple -- multiple_products	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "SQLite" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted SQL statement.	2017-05-22	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
apple_multiple_products	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "AVEVideoEncoder" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-05-22	not calcu
apple_multiple_products	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. tvOS before 10.2.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-05-22	not calcu
apple_multiple_products	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "SQLite" component. It allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a crafted SQL statement.	2017-05-22	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
apple_multiple_products	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "AVEVideoEncoder" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-05-22	not calcu
apple_multiple_products	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. iCloud before 6.2.1 on Windows is affected. tvOS before 10.2.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-05-22	not calcu
apple_multiple_products	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "AVEVideoEncoder" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-05-22	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
apple -- multiple_products	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "IOSurface" component. A race condition allows attackers to execute arbitrary code in a privileged context via a crafted app.	2017-05-22	not calcu
apple -- multiple_products	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "AVEVideoEncoder" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-05-22	not calcu
apple -- multiple_products	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. tvOS before 10.2.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-05-22	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
apple_multiple_products	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "AVEVideoEncoder" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-05-22	not calcu
apple_multiple_products	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-05-22	not calcu
apple_multiple_products	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. tvOS before 10.2.1 is affected. watchOS before 3.2.2 is affected. The issue involves the "AVEVideoEncoder" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	2017-05-22	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
apple -- safari	An issue was discovered in certain Apple products. Safari before 10.1.1 is affected. The issue involves the "Safari" component. It allows remote attackers to spoof the address bar via a crafted web site.	2017-05-22	not calcu
apple -- ios_macos	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. The issue involves the "iBooks" component. It allows attackers to execute arbitrary code in a privileged context via a crafted app that uses symlinks.	2017-05-22	not calcu
apple -- ios_macos	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. The issue involves the "SQLite" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	2017-05-22	not calcu
artifex -- ghostscript	Ghostscript before 9.21 might allow remote attackers to bypass the SAFER mode protection mechanism and consequently execute arbitrary code by leveraging type confusion in .initialize_dsc_parser.	2017-05-23	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
artifex -- ghostscript	Ghostscript before 9.21 might allow remote attackers to bypass the SAFER mode protection mechanism and consequently read arbitrary files via the use of the .libfile operator in a crafted postscript document.	2017-05-23	not calcu
artifex -- ghostscript	Use-after-free vulnerability in Ghostscript 9.20 might allow remote attackers to execute arbitrary code via vectors related to a reference leak in .setdevice.	2017-05-23	not calcu
artifex -- jbig2dec	libjbig2dec.a in Artifex jbig2dec 0.13, as used in MuPDF and Ghostscript, has a NULL pointer dereference in the jbig2_huffman_get function in jbig2_huffman.c. For example, the jbig2dec utility will crash (segmentation fault) when parsing an invalid file.	2017-05-24	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
asp.net_--_webforms_report_viewer	Cross-site scripting (XSS) vulnerability in Telerik Reporting for ASP.NET WebForms Report Viewer control before R1 2017 SP2 (11.0.17.406) allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2017-05-22	not calcu
bitcoin_project_--_bitcoin	The Bitcoin Proof-of-Work algorithm does not consider a certain attack methodology related to 80-byte block headers with a variety of initial 64-byte chunks followed by the same 16-byte chunk, multiple candidate root values ending with the same 4 bytes, and calculations involving sqrt numbers. This violates the security assumptions of (1) the choice of input, outside of the dedicated nonce area, fed into the Proof-of-Work function should not change its difficulty to evaluate and (2) every Proof-of-Work function execution should be independent.	2017-05-24	not calcu
bmw_--_330i_2011	The Bluetooth stack on the BMW 330i 2011 allows a remote crash of the CD/Multimedia software via %x or %c format string specifiers in a device name.	2017-05-23	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
bosh_director_vm	An endpoint of the Agent running on the BOSH Director VM with stemcell versions prior to 3232.6 and 3146.13 may allow unauthenticated clients to read or write blobs or cause a denial of service attack on the Director VM. This vulnerability requires that the unauthenticated clients guess or find a URL matching an existing GUID.	2017-05-25	not calcu
canonical -- juju	Juju before 1.25.12, 2.0.x before 2.0.4, and 2.1.x before 2.1.3 uses a UNIX domain socket without setting appropriate permissions, allowing privilege escalation by users on the system to root.	2017-05-27	not calcu
ceragon -- fibeair_ip-10_wireless_radios	Ceragon FibeAir IP-10 wireless radios through 7.2.0 have a default password of mateidu for the mateidu account (a hidden user account established by the vendor). This account can be accessed via both the web interface and SSH. In the web interface, this simply grants an attacker read-only access to the device's settings. However, when using SSH, this gives an attacker access to a Linux shell.	2017-05-21	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
cisco -- identity_services_engine	A vulnerability in the TCP throttling process for the GUI of the Cisco Identity Services Engine (ISE) 2.1(0.474) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device where the ISE GUI may fail to respond to new or established connection requests. The vulnerability is due to insufficient TCP rate limiting protection on the GUI. An attacker could exploit this vulnerability by sending the affected device a high rate of TCP connections to the GUI. An exploit could allow the attacker to cause the GUI to stop responding while the high rate of connections is in progress. Cisco Bug IDs: CSCvc81803.	2017-05-21	not calcu
cisco -- industrial_ethernet_1000_series_switches	A vulnerability in the Device Manager web interface of Cisco Industrial Ethernet 1000 Series Switches 1.3 could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of an affected system. The vulnerability is due to insufficient CSRF protection by the Device Manager web interface. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link or visit an attacker-controlled website. A successful exploit could allow the attacker to submit arbitrary requests to an affected device via the Device Manager web interface and with the privileges of the user. Cisco Bug IDs: CSCvc88811.	2017-05-21	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
cisco -- ip_phone	A vulnerability in the Session Initiation Protocol (SIP) implementation of Cisco IP Phone 8851 11.0(0.1) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to an abnormal SIP message. An attacker could exploit this vulnerability by manipulating the CANCEL packet. An exploit could allow the attacker to cause a disruption of service to the phone. Cisco Bug IDs: CSCvc34795.	2017-05-21	not calcu
cisco -- nx-os_system_software	A vulnerability in the Telnet CLI command of Cisco NX-OS System Software 7.1 through 7.3 running on Cisco Nexus 5000 Series Switches could allow an authenticated, local attacker to perform a command injection attack. The vulnerability is due to insufficient input validation of command arguments. An attacker could exploit this vulnerability by injecting crafted command arguments into the Telnet CLI command. An exploit could allow the attacker to read or write arbitrary files at the user's privilege level outside of the user's path. Cisco Bug IDs: CSCvb86771.	2017-05-21	not calcu
cisco -- nx-os_system_software	A vulnerability in the CLI of Cisco NX-OS System Software 7.1 through 7.3 running on Cisco Nexus 5000 Series Switches could allow an authenticated, local attacker to perform a command injection attack. The vulnerability is due to insufficient input validation of command arguments. An attacker could exploit this vulnerability by injecting crafted command arguments into a vulnerable CLI command. An exploit could allow the attacker to read or write arbitrary files at the user's privilege level outside of the user's path. Cisco Bug IDs: CSCvb86787.	2017-05-21	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
cisco -- prime_collaboration_provisioning_software	A vulnerability in the web interface of Cisco Prime Collaboration Provisioning Software (prior to Release 12.1) could allow an authenticated, remote attacker to delete any file from an affected system. The vulnerability exists because the affected software does not perform proper input validation of HTTP requests and fails to apply role-based access controls (RBACs) to requested HTTP URLs. An attacker could exploit this vulnerability by sending a crafted HTTP request that uses directory traversal techniques to submit a path to a desired file location on an affected system. A successful exploit could allow the attacker to delete any file from the system. Cisco Bug IDs: CSCvc99597.	2017-05-21	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
cisco -- prime_collaboration_provisioning_software	A vulnerability in the web interface of Cisco Prime Collaboration Provisioning Software (prior to Release 11.1) could allow an authenticated, remote attacker to delete any file from an affected system. The vulnerability exists because the affected software does not perform proper input validation of HTTP requests and fails to apply role-based access controls (RBACs) to requested HTTP URLs. An attacker could exploit this vulnerability by sending a crafted HTTP request that uses directory traversal techniques to submit a path to a desired file location on an affected system. A successful exploit could allow the attacker to delete any file from the system. Cisco Bug IDs: CSCvc99618.	2017-05-21	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
cisco_prime_collaboration_provisioning_software	A vulnerability in the web interface of Cisco Prime Collaboration Provisioning Software (prior to Release 11.1) could allow an authenticated, remote attacker to view any file on an affected system. The vulnerability exists because the affected software does not perform proper input validation of HTTP requests and fails to apply role-based access controls (RBACs) to requested HTTP URLs. An attacker could exploit this vulnerability by sending a crafted HTTP request that uses directory traversal techniques to submit a path to a desired file location on an affected system. A successful exploit could allow the attacker to view any file on the system. Cisco Bug IDs: CSCvc99604.	2017-05-21	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
cisco -- remote_expert_manager_software	A vulnerability in the web interface of Cisco Remote Expert Manager Software 11.0.0 could allow an unauthenticated, remote attacker to access sensitive information on an affected system. The vulnerability exists because the affected software does not sufficiently protect sensitive data when responding to HTTP requests that are sent to the web interface of the software. An attacker could exploit this vulnerability by sending crafted HTTP requests to the web interface of the software on an affected system. A successful exploit could allow the attacker to access sensitive information about the software. The attacker could use this information to conduct additional reconnaissance attacks. Cisco Bug IDs: CSCvc52856.	2017-05-21	not calcu
cisco -- remote_expert_manager_software	A vulnerability in the web interface of Cisco Remote Expert Manager Software 11.0.0 could allow an unauthenticated, remote attacker to access sensitive information on an affected system. The vulnerability exists because the affected software does not sufficiently protect sensitive data when responding to HTTP requests that are sent to the web interface of the software. An attacker could exploit this vulnerability by sending crafted HTTP requests to the web interface of the software on an affected system. A successful exploit could allow the attacker to access sensitive information about the software. The attacker could use this information to conduct additional reconnaissance attacks. Cisco Bug IDs: CSCvc52858.	2017-05-21	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
cisco_remote_expert_manager_software	A vulnerability in the web interface of Cisco Remote Expert Manager Software 11.0.0 could allow an unauthenticated, remote attacker to access sensitive Virtual Temporary Directory information on an affected system. The vulnerability exists because the affected software does not sufficiently protect sensitive data when responding to HTTP requests that are sent to the web interface of the software. An attacker could exploit this vulnerability by sending crafted HTTP requests to the web interface of the software on an affected system. A successful exploit could allow the attacker to access sensitive information about the software. The attacker could use this information to conduct additional reconnaissance attacks. Cisco Bug IDs: CSCvc52861.	2017-05-21	not calcu
cisco_remote_expert_manager_software	A vulnerability in the TCP connection handling functionality of Cisco Remote Expert Manager Software 11.0.0 could allow an unauthenticated, remote attacker to disable TCP ports and cause a denial of service (DoS) condition on an affected system. The vulnerability is due to a lack of rate-limiting functionality in the TCP Listen application of the affected software. An attacker could exploit this vulnerability by sending a crafted TCP traffic stream in which specific types of TCP packets are flooded to an affected device, for example a TCP packet stream in which the TCP FIN bit is set in all the TCP packets. A successful exploit could allow the attacker to cause certain TCP listening ports on the affected system to stop accepting incoming connections for a period of time or until the affected device is restarted, resulting in a DoS condition. In addition, system resources, such as CPU and memory, could be exhausted during the attack. Cisco Bug IDs: CSCva29806.	2017-05-21	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
cisco -- remote_expert_manager_software	A vulnerability in the web interface of Cisco Remote Expert Manager Software 11.0.0 could allow an unauthenticated, remote attacker to access sensitive information on an affected system. The vulnerability exists because the affected software does not sufficiently protect sensitive data when responding to HTTP requests that are sent to the web interface of the software. An attacker could exploit this vulnerability by sending crafted HTTP requests to the web interface of the software on an affected system. A successful exploit could allow the attacker to access sensitive information about the software. The attacker could use this information to conduct additional reconnaissance attacks. Cisco Bug IDs: CSCvc52860.	2017-05-21	not calcu
cisco -- remote_expert_manager_software	A vulnerability in the web interface of Cisco Remote Expert Manager Software 11.0.0 could allow an unauthenticated, remote attacker to access sensitive Temporary File information on an affected system. The vulnerability exists because the affected software does not sufficiently protect sensitive data when responding to HTTP requests that are sent to the web interface of the software. An attacker could exploit this vulnerability by sending crafted HTTP requests to the web interface of the software on an affected system. A successful exploit could allow the attacker to access sensitive information about the software. The attacker could use this information to conduct additional reconnaissance attacks. Cisco Bug IDs: CSCvc52875.	2017-05-21	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
cisco -- remote_expert_manager_software	A vulnerability in the web interface of Cisco Remote Expert Manager Software 11.0.0 could allow an unauthenticated, remote attacker to access sensitive Order information on an affected system. The vulnerability exists because the affected software does not sufficiently protect sensitive data when responding to HTTP requests that are sent to the web interface of the software. An attacker could exploit this vulnerability by sending crafted HTTP requests to the web interface of the software on an affected system. A successful exploit could allow the attacker to access sensitive information about the software. The attacker could use this information to conduct additional reconnaissance attacks. Cisco Bug IDs: CSCvc52866 CSCvc52868.	2017-05-21	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
cisco_secure_bytes_secure_cisco_auditor	Secure Bytes Cisco Configuration Manager, as bundled in Secure Bytes Secure Cisco Auditor (SCA) 3.0, has a Directory Traversal issue in its TFTP Server, allowing attackers to read arbitrary files via ../ sequences in a pathname.	2017-05-21	not calcu
cisco_ucs_c-rack_servers	A vulnerability in the TCP throttling process of Cisco UCS C-Series Rack Servers 3.0(0.234) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient rate-limiting protection. An attacker could exploit this vulnerability by sending a high rate of TCP SYN packets to a specific TCP listening port on an affected device. An exploit could allow the attacker to cause a specific TCP listening port to stop accepting new connections, resulting in a DoS condition. Cisco Bug IDs: CSCva65544.	2017-05-21	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
cisco -- unified_communications_manager	A vulnerability in the web-based management interface of Cisco Unified Communications Manager 10.5 through 11.5 could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information. Cisco Bug IDs: CSCvc06608.	2017-05-21	not calcu
contao -- contao	Directory traversal vulnerability in Contao before 3.2.19, and 3.4.x before 3.4.4 allows remote authenticated "back end" users to view files outside their file mounts or the document root via unspecified vectors.	2017-05-26	not calcu
contiki -- operating_system	An issue was discovered in Contiki Operating System 3.0. A use-after-free vulnerability exists in httpd-simple.c in cc26xx-web-demo httpd, where upon a connection close event, the http_state structure was not deallocated properly, resulting in a NULL pointer dereference in the output processing function. This resulted in a board crash, which can be used to perform denial of service.	2017-05-27	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
contiki -- operating_system	An issue was discovered in Contiki Operating System 3.0. A Persistent XSS vulnerability is present in the MQTT/IBM Cloud Config page (aka mqtt.html) of cc26xx-web-demo. The cc26xx-web-demo features a webserver that runs on a constrained device. That particular page allows a user to remotely configure that device's operation by sending HTTP POST requests. The vulnerability consists of improper input sanitisation of the text fields on the MQTT/IBM Cloud config page, allowing for JavaScript code injection.	2017-05-27	not calcu
d-link -- dir-600m	login.cgi on D-Link DIR-600M devices with firmware 3.04 allows remote attackers to bypass authentication by entering more than 20 blank spaces in the password field during an admin login attempt.	2017-05-21	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
empirical_project_monitor_extended_empirical_project_monitor_extended	Cross-site scripting vulnerability in Empirical Project Monitor - eXtended all versions allows remote authenticated attackers to inject arbitrary web script or HTML via unspecified vectors.	2017-05-22	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
empirical_project_monitor-extended--empirical_project_monitor-extended	Cross-site scripting vulnerability in Empirical Project Monitor - eXtended all versions allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2017-05-22	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
empirical_project_monitor-extended--empirical_project_monitor-extended	Untrusted search path vulnerability in Empirical Project Monitor - eXtended all versions allows remote attackers to gain privileges via a Trojan horse DLL in an unspecified directory.	2017-05-22	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
etax--etax_software	Untrusted search path vulnerability in The installer of eTax Software all versions allows remote attackers to gain privileges via a Trojan horse DLL in an unspecified directory.	2017-05-22	not calcu
evernote--evernote	Untrusted search path vulnerability in Evernote for Windows versions prior to 6.3 allows remote attackers to gain privileges via a Trojan horse DLL in an unspecified directory.	2017-05-22	not calcu
exiv2--exiv2	An issue was discovered in Exiv2 0.26. When the data structure of the structure ifd is incorrect, the program assigns pValue_ to 0x0, and the value of pValue() is 0x0. TiffImageEntry::doWriteImage will use the value of pValue() to cause a segmentation fault. To exploit this vulnerability, someone must open a crafted tiff file.	2017-05-26	not calcu
f5--big-ip	In some circumstances, an F5 BIG-IP version 12.0.0 to 12.1.2 and 13.0.0 Azure cloud instance may contain a default administrative password which could be used to remotely log into the BIG-IP system. The impacted administrative account is the Azure instance administrative user that was created at deployment. The root and admin accounts are not vulnerable. An attacker may be able to remotely access the BIG-IP host via SSH.	2017-05-23	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
fortinet -- fortianlyzer_fortimanager	An Open Redirect vulnerability in Fortinet FortiAnalyzer 5.4.0 through 5.4.2 and FortiManager 5.4.0 through 5.4.2 allows attacker to execute unauthorized code or commands via the next parameter.	2017-05-26	not calcu
fortinet -- fortios	An escalation of privilege vulnerability in Fortinet FortiClient SSL_VPN Linux versions available with FortiOS 5.4.3 and below allows an attacker to gain root privilege via the subproc file.	2017-05-26	not calcu
fortinet -- fortios	A potential execution of unauthorized code or commands vulnerability in Fortinet FortiClient SSL_VPN Linux versions available with FortiOS 5.4.2 and below allows attacker to potentially overwrite an existing file via the FortiClient log file.	2017-05-26	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
fortinet -- fortios	A stored XSS (Cross-Site-Scripting) vulnerability in Fortinet FortiOS allows attackers to execute unauthorized code or commands via the policy global-label parameter.	2017-05-23	not calcu
fortinet -- fortiportal	An open redirect vulnerability in Fortinet FortiPortal 4.0.0 and below allows attacker to execute unauthorized code or commands via the url parameter.	2017-05-26	not calcu
fortinet -- fortiportal	An improper Access Control vulnerability in Fortinet FortiPortal versions 4.0.0 and below allows an attacker to interact with unauthorized VDOMs or enumerate other ADOMs via another user's stolen session and CSRF tokens or the adomName parameter in the /fpc/sec/customer/policy/getAdomVersion request.	2017-05-26	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
fortinet -- fortiportal	A Cross-Site Scripting vulnerability in Fortinet FortiPortal versions 4.0.0 and below allows an attacker to execute unauthorized code or commands via the 'Name' and 'Description' inputs in the 'Add Revision Backup' functionality.	2017-05-26	not calcu
fortinet -- fortiportal	A password management vulnerability in Fortinet FortiPortal versions 4.0.0 and below allows an attacker to carry out information disclosure via the FortiAnalyzer Management View.	2017-05-26	not calcu
fortinet -- fortiportal	A weak password recovery vulnerability in Fortinet FortiPortal versions 4.0.0 and below allows attacker to carry out information disclosure via the Forgotten Password feature.	2017-05-26	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
fortinet -- fortiwlc-sd	An escalation of privilege vulnerability in Fortinet FortiWLC-SD versions 8.2.4 and below allows attacker to gain root access via the CLI command 'copy running-config'.	2017-05-26	not calcu
fortinet -- fortiweb	A Cross-Site Scripting vulnerability in Fortinet FortiWeb versions 5.7.1 and below allows attacker to execute unauthorized code or commands via an improperly sanitized POST parameter in the FortiWeb Site Publisher feature.	2017-05-26	not calcu
gajim -- gajim	Gajim through 0.16.7 unconditionally implements the "XEP-0146: Remote Controlling Clients" extension. This can be abused by malicious XMPP servers to, for example, extract plaintext from OTR encrypted sessions.	2017-05-27	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
gnutls_libtasn1_gnutls_libtasn1	Two errors in the "asn1_find_node()" function (lib/parser_aux.c) within GnuTLS libtasn1 version 4.10 can be exploited to cause a stacked-based buffer overflow by tricking a user into processing a specially crafted assignments file via the e.g. asn1Coding utility.	2017-05-22	not calcu
google_chrome	Use-after-free vulnerability in V8 in Google Chrome before 53.0.2785.143 allows remote attackers to cause a denial of service (crash) or possibly have unspecified other impact via unknown vectors.	2017-05-23	not calcu
google_chrome	Multiple unspecified vulnerabilities in Google Chrome before 53.0.2785.143 allow remote attackers to cause a denial of service or possibly have other impact via unknown vectors.	2017-05-23	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
hancom--thinkfree_office_neo	An exploitable heap-based buffer overflow exists in the Hangul Word Processor component (version 9.6.1.4350) of Hancom Thinkfree Office NEO 9.6.1.4902. A specially crafted document stream can cause an integer underflow resulting in a buffer overflow which can lead to code execution under the context of the application. An attacker can entice a user to open up a document in order to trigger this vulnerability.	2017-05-24	not calcu
huawei--p7_phones	The GPU driver in Huawei P7 phones with software P7-L00 before P7-L00C17B851, P7-L05 before P7-L05C00B851, and P7-L09 before P7-L09C92B851 allows local users to read or write to arbitrary kernel memory locations and consequently cause a denial of service (system crash) or gain privileges via a crafted application.	2017-05-23	not calcu
huawei--wlan_devices	The mDNS module in Huawei WLAN AC6005, AC6605, and ACU2 devices with software before V200R006C00SPC100 allows remote attackers to obtain sensitive information by leveraging failure to restrict processing of mDNS unicast queries to the link local network.	2017-05-23	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
ibm -- business_process_manager	IBM Business Process Manager 8.0 and 8.5 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 122891.	2017-05-22	not calcu
ibm -- content_navigator_cmis	IBM Content Navigator & CMIS 2.0 and 3.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 124760.	2017-05-22	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
ibm_informix_open_admin_tool	IBM Informix Open Admin Tool 11.5, 11.7, and 12.1 could allow an unauthorized user to execute arbitrary code as system admin on Windows servers. IBM X-Force ID: 120390.	2017-05-22	not calcu
ibm_inotes	IBM iNotes 8.5 and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 125976.	2017-05-26	not calcu
ibm_marketing_platform	IBM Distributed Marketing and Marketing Platform 8.6, 9.0, 9.1, and 10.0 could allow an authenticated user to escalate their privileges and gain administrative permissions over the web application. IBM X-Force ID: 118282.	2017-05-22	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
ibm -- maximo_asset_management	IBM Maximo Asset Management 7.5 and 7.6 generates error messages that could reveal sensitive information that could be used in further attacks against the system. IBM X-Force ID: 125153.	2017-05-26	not calcu
ibm -- maximo_asset_management	IBM Maximo Asset Management 7.5 and 7.6 is vulnerable to HTTP response splitting attacks. A remote attacker could exploit this vulnerability using specially-crafted URL to cause the server to return a split response, once the URL is clicked. This would allow the attacker to perform further attacks, such as Web cache poisoning, cross-site scripting, and possibly obtain sensitive information. IBM X-Force ID: 125152.	2017-05-26	not calcu
ibm -- sdk	IBM SDK, Java Technology Edition is vulnerable XML External Entity Injection (XXE) error when processing XML data. A remote attacker could exploit this vulnerability to expose highly sensitive information or consume memory resources. IBM X-Force ID: 125150.	2017-05-22	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
ibm -- tivoli_federated_identity_manager	IBM Tivoli Federated Identity Manager 6.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 125732.	2017-05-22	not calcu
imagemagick -- imagemagick_graphicsmagick	ImageMagick before 7.0.5-2 and GraphicsMagick before 1.3.24 use uninitialized memory in the RLE decoder, allowing an attacker to leak sensitive information from process memory space, as demonstrated by remote attacks against ImageMagick code in a long-running server process that converts image data on behalf of multiple users. This is caused by a missing initialization step in the ReadRLEImage function in coders/rle.c.	2017-05-19	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
imagewworsener -- imagewworsener	The iw_get_ui16le function in imagew-util.c:405:23 in libimageworsener.a in ImageWorsener 1.3.1 allows remote attackers to cause a denial of service (invalid read and SEGV) via a crafted image, related to imagew-jpeg.c.	2017-05-23	not calcu
imagewworsener -- imagewworsener	The iw_get_ui16be function in imagew-util.c:422:24 in libimageworsener.a in ImageWorsener 1.3.1 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted image, related to imagew-jpeg.c.	2017-05-23	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
imagewworsener -- imagewworsener	imagew-cmd.c:854:45 in libimageworsener.a in ImageWorsener 1.3.1 allows remote attackers to cause a denial of service (divide-by-zero error) via a crafted image, related to imagew-api.c.	2017-05-23	not calcu
imagewworsener -- imagewworsener	The iw_get_ui16le function in imagew-util.c:405:23 in libimageworsener.a in ImageWorsener 1.3.1 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted image, related to imagew-jpeg.c.	2017-05-23	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
imagewworsener -- imagewworsener	The iw_get_ui16be function in imagew-util.c:422:24 in libimageworsener.a in ImageWorsener 1.3.1 allows remote attackers to cause a denial of service (invalid read and SEGV) via a crafted image, related to imagew-jpeg.c.	2017-05-23	not calcu
imagewworsener -- imagewworsener	imagew-cmd.c:850:46 in libimageworsener.a in ImageWorsener 1.3.1 allows remote attackers to cause a denial of service (divide-by-zero error) via a crafted image, related to imagew-api.c.	2017-05-23	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
imageworsener -- imageworsener	imagew-main.c:960:12 in libimageworsener.a in ImageWorsener 1.3.1 allows remote attackers to cause a denial of service (buffer underflow) via a crafted image, related to imagew-bmp.c.	2017-05-23	not calcu
jasypt -- jasypt	jasypt before 1.9.2 allows a timing attack against the password hash comparison.	2017-05-21	not calcu
lenovo -- lenovo_solution_center	The backend service process in Lenovo Solution Center (aka LSC) before 3.3.0002 allows local users to gain SYSTEM privileges via unspecified vectors.	2017-05-23	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
libconfig-model-perl -- libconfig-model-perl	The gen_class_pod implementation in lib/Config/Model/Utils/GenClassPod.pm in Config-Model (aka libconfig-model-perl) before 2.102 has a dangerous "use lib" line, which allows remote attackers to have an unspecified impact via a crafted Debian package file.	2017-05-23	not calcu
libconfig-model-perl -- libconfig-model-perl	lib/Config/Model.pm in Config-Model (aka libconfig-model-perl) before 2.102 allows local users to gain privileges via a crafted model in the current working directory, related to use of . with the INC array.	2017-05-23	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
linux -- linux_kernel	The crypto_skcipher_init_tfm function in crypto/skcipher.c in the Linux kernel through 4.11.2 relies on a setkey function that lacks a key-size check, which allows local users to cause a denial of service (NULL pointer dereference) via a crafted application.	2017-05-23	not calcu
linux -- linux_kernel	The __ip6_append_data function in net/ipv6/ip6_output.c in the Linux kernel through 4.11.3 is too late in checking whether an overwrite of an skb data structure may occur, which allows local users to cause a denial of service (system crash) via crafted system calls.	2017-05-26	not calcu
linux -- linux	In Open vSwitch (OvS) 2.7.0, while parsing an OFPT_QUEUE_GET_CONFIG_REPLY type OFP 1.0 message, there is a buffer over-read that is caused by an unsigned integer underflow in the function `ofputil_pull_queue_get_config_reply10` in `lib/ofp-util.c`.	2017-05-23	not calcu
linux -- linux_kernel	The tcp_v6_syn_recv_sock function in net/ipv6/tcp_ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890.	2017-05-19	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
linux -- linux_kernel	The IPv6 fragmentation implementation in the Linux kernel through 4.11.1 does not consider that the nexthdr field may be associated with an invalid option, which allows local users to cause a denial of service (out-of-bounds read and BUG) or possibly have unspecified other impact via crafted socket and send system calls.	2017-05-19	not calcu
linux -- linux_kernel	The sctp_v6_create_accept_sk function in net/sctp/ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890.	2017-05-19	not calcu
linux -- linux_kernel	The dccp_v6_request_recv_sock function in net/dccp/ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890.	2017-05-19	not calcu
mantisbt -- mantisbt	MantisBT before 1.3.11, 2.x before 2.3.3, and 2.4.x before 2.4.1 omits a backslash check in string_api.php and consequently has conflicting interpretations of an initial \/ substring as introducing either a local pathname or a remote hostname, which leads to (1) arbitrary Permalink Injection via CSRF attacks on a permalink_page.php?url= URI and (2) an open redirect via a login_page.php?return= URI.	2017-05-21	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
marklogic -- marklogic	An exploitable heap overflow vulnerability exists in the ParseEnvironment functionality of AntennaHouse DMC HTMLFilter as used by MarkLogic 8.0-6.	2017-05-23	not calcu
marklogic -- marklogic	An exploitable heap corruption vulnerability exists in the UnCompressUnicode functionality of Antenna House DMC HTMLFilter used by MarkLogic 8.0-6. A specially crafted xls file can cause a heap corruption resulting in arbitrary code execution. An attacker can send/provide malicious XLS file to trigger this vulnerability.	2017-05-23	not calcu
marklogic -- marklogic	An exploitable heap corruption vulnerability exists in the FillRowFormat functionality of Antenna House DMC HTMLFilter that is shipped with MarkLogic 8.0-6. A specially crafted xls file can cause a heap corruption resulting in arbitrary code execution. An attacker can send/provide malicious xls file to trigger this vulnerability.	2017-05-23	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
marklogic -- marklogic	An exploitable stack-based buffer overflow vulnerability exists in the DHFSummary functionality of AntennaHouse DMC HTMLFilter as used by MarkLogic 8.0-6. A specially crafted PPT file can cause a stack corruption resulting in arbitrary code execution. An attacker can send/provide malicious PPT file to trigger this vulnerability.	2017-05-23	not calcu
marklogic -- marklogic	An exploitable heap corruption vulnerability exists in the GetIndexArray functionality of Antenna House DMC HTMLFilter as used by MarkLogic 8.0-6. A specially crafted XLS file can cause a heap corruption resulting in arbitrary code execution. An attacker can send or provide a malicious XLS file to trigger this vulnerability.	2017-05-24	not calcu
marklogic -- marklogic	An exploitable heap corruption vulnerability exists in the AddSst functionality of Antenna House DMC HTMLFilter as used by MarkLogic 8.0-6. A specially crafted XLS file can cause a heap corruption resulting in arbitrary code execution. An attacker can send or provide a malicious XLS file to trigger this vulnerability.	2017-05-24	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
metadata_anonymisation_toolkit -- metadata_anonymisation_toolkit	Metadata Anonymisation Toolkit (MAT) 0.6 and 0.6.1 silently fails to perform "Clean metadata" actions upon invocation from the Nautilus contextual menu, which allows context-dependent attackers to obtain sensitive information by reading a file for which cleaning had been attempted.	2017-05-22	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
microsoft -- multiple_products	The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to denial of service. aka "Microsoft Malware Protection Engine Denial of Service Vulnerability", a different vulnerability than CVE-2017-8535, CVE-2017-8536, CVE-2017-8537, and CVE-2017-8539.	2017-05-26	not calcu
microsoft -- multiple_products	The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to memory corruption. aka "Microsoft Malware Protection Engine Remote Code Execution Vulnerability", a different vulnerability than CVE-2017-8538 and CVE-2017-8540.	2017-05-26	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
microsoft_multiple_products	The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to denial of service. aka "Microsoft Malware Protection Engine Denial of Service Vulnerability", a different vulnerability than CVE-2017-8535, CVE-2017-8537, CVE-2017-8539, and CVE-2017-8542.	2017-05-26	not calcu
microsoft_multiple_products	The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to denial of service. aka "Microsoft Malware Protection Engine Denial of Service Vulnerability", a different vulnerability than CVE-2017-8536, CVE-2017-8537, CVE-2017-8539, and CVE-2017-8542.	2017-05-26	not calcu

Primary Vendor -- Product	Description	Published	CVSS Sco
microsoft -- multiple_products	The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to memory corruption. aka "Microsoft Malware Protection Engine Remote Code Execution Vulnerability", a different vulnerability than CVE-2017-8538 and CVE-2017-8541.	2017-05-26	not calcu
microsoft -- multiple_products	The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to denial of service. aka "Microsoft Malware Protection Engine Denial of Service Vulnerability", a different vulnerability than CVE-2017-8535, CVE-2017-8536, CVE-2017-8537, and CVE-2017-8542.	2017-05-26	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
microsoft -- multiple_products	The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to denial of service. aka "Microsoft Malware Protection Engine Denial of Service Vulnerability", a different vulnerability than CVE-2017-8535, CVE-2017-8536, CVE-2017-8539, and CVE-2017-8542.	2017-05-26	not calcu
microsoft -- multiple_products	The Microsoft Malware Protection Engine running on Microsoft Forefront and Microsoft Defender on Microsoft Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016, Microsoft Exchange Server 2013 and 2016, does not properly scan a specially crafted file leading to memory corruption. aka "Microsoft Malware Protection Engine Remote Code Execution Vulnerability", a different vulnerability than CVE-2017-8540 and CVE-2017-8541.	2017-05-26	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
netapp -- oncommand_unified_manager_core_package	SQL injection vulnerability in NetApp OnCommand Unified Manager Core Package 5.x before 5.2.2P1 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	2017-05-25	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
netapp -- oncommand_unified_manager_core_package	NetApp OnCommand Unified Manager Core Package 5.x before 5.2.2P1 might allow remote attackers to obtain sensitive information via vectors involving error messages.	2017-05-25	not calcu
netcar -- wnr2000_devices	NETGEAR WNR2000v3 devices before 1.1.2.14, WNR2000v4 devices before 1.0.0.66, and WNR2000v5 devices before 1.0.0.42 allow authentication bypass and remote code execution via a buffer overflow that uses a parameter in the administration webapp. The NETGEAR ID is PSV-2016-0261.	2017-05-26	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
ntt_docomo--l-04d	Cross-site request forgery (CSRF) vulnerability in L-04D firmware version V10a and V10b allows remote attackers to hijack the authentication of administrators to perform arbitrary operations via unspecified vectors.	2017-05-22	not calcu
oniguruma--oniguruma	An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A SIGSEGV occurs in left_adjust_char_head() during regular expression compilation. Invalid handling of reg->dmax in forward_search_range() could result in an invalid pointer dereference, normally as an immediate denial-of-service condition.	2017-05-24	not calcu
oniguruma--oniguruma	An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A heap out-of-bounds write or read occurs in next_state_val() during regular expression compilation. Octal numbers larger than 0xff are not handled correctly in fetch_token() and fetch_token_in_cc(). A malformed regular expression containing an octal number in the form of '\700' would produce an invalid code point value larger than 0xff in next_state_val(), resulting in an out-of-bounds write memory corruption.	2017-05-24	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
oniguruma -- oniguruma	An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A heap out-of-bounds write occurs in bitset_set_range() during regular expression compilation due to an uninitialized variable from an incorrect state transition. An incorrect state transition in parse_char_class() could create an execution path that leaves a critical local variable uninitialized until it's used as an index, resulting in an out-of-bounds write memory corruption.	2017-05-24	not calcu
oniguruma -- oniguruma	An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A stack out-of-bounds read occurs in match_at() during regular expression searching. A logical error involving order of validation and access in match_at() could result in an out-of-bounds read from a stack buffer.	2017-05-24	not calcu
oniguruma -- oniguruma	An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A stack out-of-bounds write in onigenc_unicode_get_case_fold_codes_by_str() occurs during regular expression compilation. Code point 0xFFFFFFFF is not properly handled in unicode_unfold_key(). A malformed regular expression could result in 4 bytes being written off the end of a stack buffer of expand_case_fold_string() during the call to onigenc_unicode_get_case_fold_codes_by_str(), a typical stack buffer overflow.	2017-05-24	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
oniguruma -- oniguruma	An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A stack out-of-bounds read occurs in mbc_enc_len() during regular expression searching. Invalid handling of reg->dmin in forward_search_range() could result in an invalid pointer dereference, as an out-of-bounds read from a stack buffer.	2017-05-24	not calcu
open_source_solutions -- vimbadmin	Multiple cross-site scripting (XSS) vulnerabilities in ViMbAdmin 3.0.15 allow remote attackers to inject arbitrary web script or HTML via the (1) domain or (2) transport parameter to domain/add; the (3) name parameter to mailbox/add/did/<domain id>; the (4) goto parameter to alias/add/did/<domain id>; or the (5) captchatext parameter to auth/lost-password.	2017-05-23	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
openvpn_access_server	CRLF injection vulnerability in the web interface in OpenVPN Access Server 2.1.4 allows remote attackers to inject arbitrary HTTP headers and consequently conduct session fixation attacks and possibly HTTP response splitting attacks via "%0A" characters in the PATH_INFO to __session_start__/.	2017-05-25	not calcu
openexr -- openexr	In OpenEXR 2.2.0, an invalid read of size 1 in the refill function in ImfFastHuf.cpp could cause the application to crash.	2017-05-21	not calcu
openexr -- openexr	In OpenEXR 2.2.0, an invalid read of size 2 in the hufDecode function in ImfHuf.cpp could cause the application to crash.	2017-05-21	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
openexr -- openexr	In OpenEXR 2.2.0, an invalid read of size 1 in the getBits function in ImfHuf.cpp could cause the application to crash.	2017-05-21	not calcu
openexr -- openexr	In OpenEXR 2.2.0, an invalid write of size 8 in the storeSSE function in ImfOptimizedPixelReading.h could cause the application to crash or execute arbitrary code.	2017-05-21	not calcu
openexr -- openexr	In OpenEXR 2.2.0, an invalid write of size 2 in the = operator function in half.h could cause the application to crash or execute arbitrary code.	2017-05-21	not calcu
openexr -- openexr	In OpenEXR 2.2.0, an invalid read of size 1 in the uncompress function in ImfZip.cpp could cause the application to crash.	2017-05-21	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
openexr -- openexr	In OpenEXR 2.2.0, an invalid write of size 1 in the bufferedReadPixels function in ImfInputFile.cpp could cause the application to crash or execute arbitrary code.	2017-05-21	not calcu
pegasus_mail -- pegasus_mail	winpm-32.exe in Pegasus Mail (aka Pmail) v4.72 build 572 allows code execution via a crafted ssgp.dll file that must be installed locally. For example, if ssgp.dll is on the desktop and executes arbitrary code in the DllMain function, then clicking on a mailto: link on a remote web page triggers the attack.	2017-05-21	not calcu
pgbouncer -- pgbouncer	PgBouncer 1.6.x before 1.6.1, when configured with auth_user, allows remote attackers to gain login access as auth_user via an unknown username.	2017-05-23	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
pgbouncer -- pgbouncer	PgBouncer before 1.5.5 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) by sending a password packet before a startup packet.	2017-05-23	not calcu
php -- php	The i_zval_ptr_dtor function in Zend/zend_variables.h in PHP 7.1.5 allows attackers to cause a denial of service (memory consumption and application crash) or possibly have unspecified other impact by triggering crafted operations on array data structures.	2017-05-21	not calcu
picocom -- picocom	picocom before 2.0 has a command injection vulnerability in the 'send and receive file' command because the command line is executed by /bin/sh unsafely.	2017-05-27	not calcu
pivotal_cloud_foundry	A path traversal vulnerability was identified in the Cloud Foundry component Cloud Controller that affects cf-release versions prior to v208 and Pivotal Cloud Foundry Elastic Runtime versions prior to 1.4.2. Path traversal is the 'outbreak' of a given directory structure through relative file paths in the user input. It aims at accessing files and directories that are stored outside the web root folder, for disallowed reading or even executing arbitrary system commands. An attacker could use a certain parameter of the file path for instance to inject '../' sequences in order to navigate through the file system. In this particular case a remote authenticated attacker can exploit the identified vulnerability in order to upload arbitrary files to the server running a Cloud Controller instance - outside the isolated application container.	2017-05-25	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
pivotal_cloud_foundry	It was discovered that cf-release v231 and lower, Pivotal Cloud Foundry Elastic Runtime 1.5.x versions prior to 1.5.17 and Pivotal Cloud Foundry Elastic Runtime 1.6.x versions prior to 1.6.18 do not properly enforce disk quotas in certain cases. An attacker could use an improper disk quota value to bypass enforcement and consume all the disk on DEAs/CELLs causing a potential denial of service for other applications.	2017-05-25	not calcu
pivotal_cloud_foundry	With Cloud Foundry Runtime cf-release versions v209 or earlier, UAA Standalone versions 2.2.6 or earlier and Pivotal Cloud Foundry Runtime 1.4.5 or earlier the UAA logout link is susceptible to an open redirect which allows an attacker to insert malicious web page as a redirect parameter.	2017-05-25	not calcu
pivotal_cloud_foundry	Cloud Foundry Garden-Linux versions prior to v0.333.0 and Elastic Runtime 1.6.x version prior to 1.6.17 contain a flaw in managing container files during Docker image preparation that could be used to delete, corrupt or overwrite host files and directories, including other container filesystems on the host.	2017-05-25	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
pivotal_cloud_foundry	The UAA OAuth approval pages in Cloud Foundry v208 to v231, Login-server v1.6 to v1.14, UAA v2.0.0 to v2.7.4.1, UAA v3.0.0 to v3.2.0, UAA-Release v2 to v7 and Pivotal Elastic Runtime 1.6.x versions prior to 1.6.20 are vulnerable to an XSS attack by specifying malicious java script content in either the OAuth scopes (SCIM groups) or SCIM group descriptions.	2017-05-25	not calcu
pivotal_cloud_foundry	With Cloud Foundry Runtime cf-release versions v209 or earlier, UAA Standalone versions 2.2.6 or earlier and Pivotal Cloud Foundry Runtime 1.4.5 or earlier the change_email form in UAA is vulnerable to a CSRF attack. This allows an attacker to trigger an e-mail change for a user logged into a cloud foundry instance via a malicious link on a attacker controlled site. This vulnerability is applicable only when using the UAA internal user store for authentication. Deployments enabled for integration via SAML or LDAP are not affected.	2017-05-25	not calcu
pivotal_cloud_foundry	With Cloud Foundry Runtime cf-release versions v208 or earlier, UAA Standalone versions 2.2.5 or earlier and Pivotal Cloud Foundry Runtime 1.4.5 or earlier, old Password Reset Links are not expired after the user changes their current email address to a new one. This vulnerability is applicable only when using the UAA internal user store for authentication. Deployments enabled for integration via SAML or LDAP are not affected.	2017-05-25	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
pivotal_spring_framework	Under some situations, the Spring Framework 4.2.0 to 4.2.1, 4.0.0 to 4.1.7, 3.2.0 to 3.2.14 and older unsupported versions is vulnerable to a Reflected File Download (RFD) attack. The attack involves a malicious user crafting a URL with a batch script extension that results in the response being downloaded rather than rendered and also includes some input reflected in the response.	2017-05-25	not calcu
pivotal_spring_framework	When processing user provided XML documents, the Spring Framework 4.0.0 to 4.0.4, 3.0.0 to 3.2.8, and possibly earlier unsupported versions did not disable by default the resolution of URI references in a DTD declaration. This enabled an XXE attack.	2017-05-25	not calcu
pivotal_spring_security	When processing authorization requests using the whitelabel views in Spring Security OAuth 2.0.0 to 2.0.9 and 1.0.0 to 1.0.5, the response_type parameter value was executed as Spring SpEL which enabled a malicious user to trigger remote code execution via the crafting of the value for response_type.	2017-05-25	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
pivotal_software -- spring_security	Both Spring Security 3.2.x, 4.0.x, 4.1.0 and the Spring Framework 3.2.x, 4.0.x, 4.1.x, 4.2.x rely on URL pattern mappings for authorization and for mapping requests to controllers respectively. Differences in the strictness of the pattern matching mechanisms, for example with regards to space trimming in path segments, can lead Spring Security to not recognize certain paths as not protected that are in fact mapped to Spring MVC controllers that should be protected. The problem is compounded by the fact that the Spring Framework provides richer features with regards to pattern matching as well as by the fact that pattern matching in each Spring Security and the Spring Framework can easily be customized creating additional differences.	2017-05-25	not calcu
pivotal_software -- spring_security	The ActiveDirectoryLdapAuthenticator in Spring Security 3.2.0 to 3.2.1 and 3.1.0 to 3.1.5 does not check the password length. If the directory allows anonymous binds then it may incorrectly authenticate a user who supplies an empty password.	2017-05-25	not calcu
pivotal_software -- spring_security	When using the CAS Proxy ticket authentication from Spring Security 3.1 to 3.2.4 a malicious CAS Service could trick another CAS Service into authenticating a proxy ticket that was not associated. This is due to the fact that the proxy ticket authentication uses the information from the HttpServletRequest which is populated based upon untrusted information within the HTTP request. This means if there are access control restrictions on which CAS services can authenticate to one another, those restrictions can be bypassed. If users are not using CAS Proxy tickets and not basing access control decisions based upon the CAS Service, then there is no impact to users.	2017-05-25	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
pivotal_cloudfoundry	The UAA reset password flow in Cloud Foundry release v236 and earlier versions, UAA release v3.3.0 and earlier versions, all versions of Login-server, UAA release v10 and earlier versions and Pivotal Elastic Runtime versions prior to 1.7.2 is vulnerable to a brute force attack due to multiple active codes at a given time. This vulnerability is applicable only when using the UAA internal user store for authentication. Deployments enabled for integration via SAML or LDAP are not affected.	2017-05-25	not calcu
pivotal_cloudfoundry	The Loggregator Traffic Controller endpoints in cf-release v231 and lower, Pivotal Elastic Runtime versions prior to 1.5.19 AND 1.6.x versions prior to 1.6.20 are not cleansing request URL paths when they are invalid and are returning them in the 404 response. This could allow malicious scripts to be written directly into the 404 response.	2017-05-25	not calcu
playsms -- playsms	import.php (aka the Phonebook import feature) in PlaySMS 1.4 allows remote code execution via vectors involving the User-Agent HTTP header and PHP code in the name of a file.	2017-05-21	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
pngquant -- pngquant	Integer overflow in the rwpng_read_image24_libpng function in rwpng.c in pngquant 2.7.0 allows remote attackers to have unspecified impact via a crafted PNG file, which triggers a buffer overflow.	2017-05-23	not calcu
power_software -- poweriso	A use-after-free vulnerability exists in the .ISO parsing functionality of PowerISO 6.8. A specially crafted .ISO file can cause a vulnerability resulting in potential code execution. An attacker can send a specific .ISO file to trigger this vulnerability.	2017-05-24	not calcu
power_software -- poweriso	A stack buffer overflow vulnerability exists in the ISO parsing functionality of Power Software Ltd PowerISO 6.8. A specially crafted ISO file can cause a vulnerability resulting in potential code execution. An attacker can send a specific ISO file to trigger this vulnerability.	2017-05-24	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
qemu -- qemu	Memory leak in the keyboard input event handlers support in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (host memory consumption) by rapidly generating large keyboard events.	2017-05-23	not calcu
qemu -- qemu	Memory leak in the audio/audio.c in QEMU (aka Quick Emulator) allows remote attackers to cause a denial of service (memory consumption) by repeatedly starting and stopping audio capture.	2017-05-23	not calcu
qpdf -- qpdf	libqpdf.a in QPDF 6.0.0 allows remote attackers to cause a denial of service (infinite recursion and stack consumption) via a crafted PDF document, related to releaseResolved functions, aka qpdf-infiniteloop1.	2017-05-23	not calcu
qpdf -- qpdf	libqpdf.a in QPDF 6.0.0 allows remote attackers to cause a denial of service (infinite recursion and stack consumption) via a crafted PDF document, related to QPDFObjectHandle::parseInternal, aka qpdf-infiniteloop2.	2017-05-23	not calcu
qpdf -- qpdf	libqpdf.a in QPDF 6.0.0 allows remote attackers to cause a denial of service (infinite recursion and stack consumption) via a crafted PDF document, related to unparse functions, aka qpdf-infiniteloop3.	2017-05-23	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
randombit_botan -- randombit_botan	A programming error exists in a way Randombit Botan cryptographic library version 2.0.1 implements x500 string comparisons which could lead to certificate verification issues and abuse. A specially crafted X509 certificate would need to be delivered to the client or server application in order to trigger this vulnerability.	2017-05-24	not calcu
red_hat -- jboss_application_server	HTTPServerILServlet.java in JMS over HTTP Invocation Layer of the JbossMQ implementation, which is enabled by default in Red Hat Jboss Application Server <= Jboss 4.X does not restrict the classes for which it performs deserialization, which allows remote attackers to execute arbitrary code via crafted serialized data.	2017-05-19	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
redmine -- redmine	Cross-site scripting (XSS) vulnerability in Redmine before 2.6.2 allows remote attackers to inject arbitrary web script or HTML via vectors involving flash message rendering.	2017-05-23	not calcu
roundcube -- roundcube_webmail	program/steps/addressbook/photo.inc in Roundcube Webmail before 1.0.6 and 1.1.x before 1.1.2 allows remote authenticated users to read arbitrary files via the _alt parameter when uploading a vCard.	2017-05-23	not calcu
roundcube -- roundcube_webmail	Roundcube Webmail 1.1.x before 1.1.2 allows remote attackers to obtain sensitive information by reading files in the (1) config, (2) temp, or (3) logs directory.	2017-05-23	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
roundcube -- roundcube_webmail	Cross-site scripting (XSS) vulnerability in program/include/rcmail.php in Roundcube Webmail 1.1.x before 1.1.2 allows remote attackers to inject arbitrary web script or HTML via the _mbox parameter to the default URI.	2017-05-23	not calcu
sap -- business_one_for_android	SAP Business One for Android 1.2.3 allows remote attackers to conduct XML External Entity (XXE) attacks via crafted XML data in a request to B1iXcellerator/exec/soap/vP.001sap0003.in_WCSX/com.sap.b1i.vplatform.runtime/INB_WS_CALL_SYNC_XPT/INB_WS_CALL_SYNC_XPT.ipo/proc, aka SAP Security Note 2378065.	2017-05-25	not calcu
sap -- hana_xs	sinopia, as used in SAP HANA XS 1.00 and 2.00, allows remote attackers to hijack npm packages or host arbitrary files by leveraging an insecure user creation policy, aka SAP Security Note 2407694.	2017-05-23	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
sap_hana_xs	sinopia, as used in SAP HANA XS 1.00 and 2.00, allows remote attackers to cause a denial of service (assertion failure and service crash) by pushing a package with a filename containing a $ (dollar sign) or % (percent) character, aka SAP Security Note 2407694.	2017-05-23	not calcu
sap_netweaver_as_java	The Visual Composer VC70RUNTIME component in SAP NetWeaver AS JAVA 7.5 allows remote authenticated users to conduct XML External Entity (XXE) attacks via a crafted XML document in a request to irj/servlet/prt/portal/prtroot/com.sap.visualcomposer.BIKit.default, aka SAP Security Note 2386873.	2017-05-23	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
schneider_electric--wonderware_indusoft_web_studio	An Incorrect Default Permissions issue was discovered in Schneider Electric Wonderware InduSoft Web Studio v8.0 Patch 3 and prior versions. Upon installation, Wonderware InduSoft Web Studio creates a new directory and two files, which are placed in the system's path and can be manipulated by non-administrators. This could allow an authenticated user to escalate his or her privileges.	2017-05-19	not calcu
sitecore--crm	Sitecore CRM 8.1 Rev 151207 allows remote authenticated administrators to read arbitrary files via an absolute path traversal attack on sitecore/shell/download.aspx with the file parameter.	2017-05-23	not calcu
sitecore--crm	The package manager in Sitecore CRM 8.1 Rev 151207 allows remote authenticated administrators to execute arbitrary ASP code by creating a ZIP archive in which a .asp file has a ..\ in its pathname, visiting sitecore/shell/applications/install/dialogs/Upload%20Package/UploadPackage2.aspx to upload this archive and extract its contents, and visiting a URI under sitecore/ to execute the .asp file.	2017-05-23	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
synacore -- zimbra_collaboration_suite	Cross-site scripting (XSS) vulnerability in Zimbra Collaboration Suite (ZCS) before 8.7.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2017-05-23	not calcu
synacore -- zimbra_collaboration_suite	A service provided by Zimbra Collaboration Suite (ZCS) before 8.7.6 fails to require needed privileges before performing a few requested operations.	2017-05-23	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
synacor -- zimbra_collaboration_suite	Directory traversal vulnerability in Zimbra Collaboration Suite (aka ZCS) before 8.7.6 allows attackers to have unspecified impact via unknown vectors.	2017-05-23	not calcu
systemd -- systemd-resolved	systemd-resolved through 233 allows remote attackers to cause a denial of service (daemon crash) via a crafted DNS response with an empty question section.	2017-05-24	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
tenda -- routers	There is a debug-interface vulnerability on some Tenda routers (FH1202/F1202/F1200: versions before 1.2.0.20). After connecting locally to a router in a wired or wireless manner, one can bypass intended access restrictions by sending shell commands directly and reading their results, or by entering shell commands that change this router's username and password.	2017-05-21	not calcu
tenda -- routers	There is a stack-based buffer overflow on some Tenda routers (FH1202/F1202/F1200: versions before 1.2.0.20). Crafted POST requests to an unspecified URL result in DoS, interrupting the HTTP service (used to login to the web UI of a router) for 1 to 2 seconds.	2017-05-21	not calcu
teradata -- teradata_gateway	Teradata Gateway before 15.00.03.02-1 and 15.10.x before 15.10.00.01-1 and TD Express before 15.00.02.08 Sles10 and 15.00.02.08 Sles11 allow remote attackers to cause a denial of service (database crash) via a malformed CONFIG REQUEST message.	2017-05-23	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
the_foreman--the_foreman	Foreman since version 1.5 is vulnerable to an incorrect authorization check due to which users with user management permission who are assigned to some organization(s) can do all operations granted by these permissions on all administrator user object outside of their scope, such as editing global admin accounts including changing their passwords.	2017-05-26	not calcu
toshiba--flashair_sdhc_memory_card	FlashAirTM SDHC Memory Card (SD-WE Series <W-03>) V3.00.02 and earlier and FlashAirTM SDHC Memory Card (SD-WD/WC Series <W-02>) V2.00.04 and earlier allows default credentials to be set for wireless LAN connections to the product when enabling the PhotoShare function through a web browser.	2017-05-22	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
toshiba -- flashair_sdhc_memory_card	FlashAirTM SDHC Memory Card (SD-WE Series <W-03>) V3.00.02 and earlier and FlashAirTM SDHC Memory Card (SD-WD/WC Series <W-02>) V2.00.04 and earlier allows authenticated attackers to bypass access restrictions to obtain unauthorized image data via unspecified vectors.	2017-05-22	not calcu
toshiba -- flashair	The Toshiba FlashAir SD-WD/WC series Class 6 model with firmware version 1.00.04 and later, FlashAir SD-WD/WC series Class 10 model W-02 with firmware version 2.00.02 and later, FlashAir SD-WE series Class 10 model W-03, FlashAir Class 6 model with firmware version 1.00.04 and later, FlashAir II Class 10 model W-02 series with firmware version 2.00.02 and later, FlashAir III Class 10 model W-03 series, FlashAir Class 6 model with firmware version 1.00.04 and later, FlashAir W-02 series Class 10 model with firmware version 2.00.02 and later, FlashAir W-03 series Class 10 model does not require authentication on accepting a connection from STA side LAN when "Internet pass-thru Mode" is enabled, which allows attackers with access to STA side LAN can obtain files or data.	2017-05-22	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
trend_micro--server_protect_for_linux	Multiple cross-site scripting (XSS) vulnerabilities in Trend Micro ServerProtect for Linux 3.0 before CP 1531 allow remote attackers to inject arbitrary web script or HTML via the (1) S44, (2) S5, (3) S_action_fail, (4) S_ptn_update, (5) T113, (6) T114, (7) T115, (8) T117117, (9) T118, (10) T_action_fail, (11) T_ptn_update, (12) textarea, (13) textfield5, or (14) tmLastConfigFileModifiedDate parameter to notification.cgi.	2017-05-25	not calcu
trend_micro--server_protect_for_linux	Multiple cross-site scripting (XSS) vulnerabilities in Trend Micro ServerProtect for Linux 3.0 before CP 1531 allow remote attackers to inject arbitrary web script or HTML via the (1) T1 or (2) tmLastConfigFileModifiedDate parameter to log_management.cgi.	2017-05-25	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
trend_micro--server_protect_for_linux	Cross-site request forgery (CSRF) vulnerability in Trend Micro ServerProtect for Linux 3.0 before CP 1531 allows remote attackers to hijack the authentication of users for requests to start an update from an arbitrary source via a crafted request to SProtectLinux/scanoption_set.cgi, related to the lack of anti-CSRF tokens.	2017-05-25	not calcu
trend_micro--server_protect_for_linux	Trend Micro ServerProtect for Linux 3.0 before CP 1531 allows local users to gain privileges by leveraging an unrestricted quarantine directory.	2017-05-25	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
trend_micro--server_protect_for_linux	Trend Micro ServerProtect for Linux 3.0 before CP 1531 allows attackers to eavesdrop and tamper with updates by leveraging unencrypted communications with update servers.	2017-05-25	not calcu
trend_micro--server_protect_for_linux	Trend Micro ServerProtect for Linux 3.0 before CP 1531 allows attackers to write to arbitrary files and consequently execute arbitrary code with root privileges by leveraging failure to validate software updates.	2017-05-25	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
vanilla_forums -- vanilla_forums	The from method in library/core/class.email.php in Vanilla Forums before 2.3.1 allows remote attackers to spoof the email domain in sent messages and potentially obtain sensitive information via a crafted HTTP Host header, as demonstrated by a password reset request.	2017-05-23	not calcu
videolan_vlc -- videolan_vlc	Heap out-of-bound read in ParseJSS in VideoLAN VLC due to missing check of string length allows attackers to read heap uninitialized data via a crafted subtitles file.	2017-05-23	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
videolan_vlc -- videolan_vlc	Potential heap based buffer overflow in ParseJSS in VideoLAN VLC before 2.2.5 due to skipping NULL terminator in an input string allows attackers to execute arbitrary code via a crafted subtitles file.	2017-05-23	not calcu
videolan_vlc -- videolan_vlc	Heap out-of-bound read in CreateHtmlSubtitle in VideoLAN VLC 2.2.x due to missing check of string termination allows attackers to read data beyond allocated memory and potentially crash the process (causing a denial of service) via a crafted subtitles file.	2017-05-23	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
videolan_vlc -- videolan_vlc	Heap out-of-bound read in ParseJSS in VideoLAN VLC before 2.2.5 due to missing check of string termination allows attackers to read data beyond allocated memory and potentially crash the process via a crafted subtitles file.	2017-05-23	not calcu
virgl -- virglrenderer	The vrend_clear dispatch function in vrend_renderer.c in virglrenderer before 0.6.0 allows local guest OS users to cause a denial of service (NULL pointer dereference) via a crafted value in "buffers."	2017-05-26	not calcu
vmware -- workstation_pro/player	VMware Workstation Pro/Player contains a NULL pointer dereference vulnerability that exists in the vstor2 driver. Successful exploitation of this issue may allow host users with normal user privileges to trigger a denial-of-service in a Windows host machine.	2017-05-22	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
vmware_workstation_pro/player	VMware Workstation Pro/Player contains an insecure library loading vulnerability via ALSA sound driver configuration files. Successful exploitation of this issue may allow unprivileged host users to escalate their privileges to root in a Linux host machine.	2017-05-22	not calcu
wolfssl -- wolfssl	A specially crafted x509 certificate can cause a single out of bounds byte overwrite in wolfSSL through 3.10.2 resulting in potential certificate validation vulnerabilities, denial of service and possible remote code execution. In order to trigger this vulnerability, the attacker needs to supply a malicious x509 certificate to either a server or a client application using this library.	2017-05-24	not calcu
wordpress -- wordpress	Cross-site scripting vulnerability in WP Booking System Free version prior to version 1.4 and WP Booking System Premium version prior to version 3.7 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2017-05-22	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
wordpress -- wordpress	Absolute path traversal vulnerability in the Image Export plugin 1.1 for WordPress allows remote attackers to read and delete arbitrary files via a full pathname in the file parameter to download.php.	2017-05-23	not calcu
wordpress -- wordpress	upload.php in the Powerplay Gallery plugin 3.3 for WordPress allows remote attackers to create arbitrary directories via vectors related to the targetDir variable.	2017-05-23	not calcu
wordpress -- wordpress	Absolute path traversal vulnerability in the MDC YouTube Downloader plugin 2.1.0 for WordPress allows remote attackers to read arbitrary files via a full pathname in the file parameter to includes/download.php.	2017-05-23	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
wordpress -- wordpress	Directory traversal vulnerability in the Download Zip Attachments plugin 1.0 for WordPress allows remote attackers to read arbitrary files via a .. (dot dot) in the File parameter to download.php.	2017-05-23	not calcu
wordpress -- wordpress	Cross-site scripting vulnerability in MaxButtons prior to version 6.19 and MaxButtons Pro prior to version 6.19 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2017-05-22	not calcu
wordpress -- wordpress	Directory traversal vulnerability in the WP e-Commerce Shop Styling plugin before 2.6 for WordPress allows remote attackers to read arbitrary files via a .. (dot dot) in the filename parameter to includes/download.php.	2017-05-23	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
wordpress -- wordpress	Cross-site scripting vulnerability in Captcha prior to version 4.3.0, Car Rental prior to version 1.0.5, Contact Form Multi prior to version 1.2.1, Contact Form prior to version 4.0.6, Contact Form to DB prior to version 1.5.7, Custom Admin Page prior to version 0.1.2, Custom Fields Search prior to version 1.3.2, Custom Search prior to version 1.36, Donate prior to version 2.1.1, Email Queue prior to version 1.1.2, Error Log Viewer prior to version 1.0.6, Facebook Button prior to version 2.54, Featured Posts prior to version 1.0.1, Gallery Categories prior to version 1.0.9, Gallery prior to version 4.5.0, Google +1 prior to version 1.3.4, Google AdSense prior to version 1.44, Google Analytics prior to version 1.7.1, Google Captcha (reCAPTCHA) prior to version 1.28, Google Maps prior to version 1.3.6, Google Shortlink prior to version 1.5.3, Google Sitemap prior to version 3.0.8, Htaccess prior to version 1.7.6, Job Board prior to version 1.1.3, Latest Posts prior to version 0.3, Limit Attempts prior to version 1.1.8, LinkedIn prior to version 1.0.5, Multilanguage prior to version 1.2.2, PDF & Print prior to version 1.9.4, Pagination prior to version 1.0.7, Pinterest prior to version 1.0.5, Popular Posts prior to version 1.0.5, Portfolio prior to version 2.4, Post to CSV prior to version 1.3.1, Profile Extra prior to version 1.0.7. PromoBar prior to version 1.1.1, Quotes and Tips prior to version 1.32, Re-attacher prior to version 1.0.9, Realty prior to version 1.1.0, Relevant - Related Posts prior to version 1.2.0, Sender prior to version 1.2.1, SMTP prior to version 1.1.0, Social Buttons Pack prior to version 1.1.1, Subscriber prior to version 1.3.5, Testimonials prior to version 0.1.9, Timesheet prior to version 0.1.5, Twitter Button prior to version 2.55, User Role prior to version 1.5.6, Updater prior to version 1.35, Visitors Online prior to version 1.0.0, and Zendesk Help Center prior to version 1.0.5 allows remote attackers to inject arbitrary web script or HTML via the function to display the BestWebSoft menu.	2017-05-22	not calcu
wordpress -- wordpress	Unrestricted file upload vulnerability in includes/upload.php in the Aviary Image Editor Add-on For Gravity Forms plugin 3.0 beta for WordPress allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in wp-content/uploads/gform_aviary.	2017-05-23	not calcu
wordpress -- wp-olivecart	SQL injection vulnerability in the WP-OliveCart versions prior to 3.1.3 and WP-OliveCartPro versions prior to 3.1.8 allows attackers with administrator rights to execute arbitrary SQL commands via unspecified vectors.	2017-05-22	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
wordpress -- wp-olivecart	Cross-site request forgery (CSRF) vulnerability in WP-OliveCart versions prior to 3.1.3 and WP-OliveCartPro versions prior to 3.1.8 allows remote attackers to hijack the authentication of a user to perform unintended operations via unspecified vectors.	2017-05-22	not calcu
wordpress -- wp-olivecart	Cross-site scripting vulnerability in WP-OliveCart versions prior to 3.1.3 and WP-OliveCartPro versions prior to 3.1.8 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2017-05-22	not calcu
xbmc/kodi_foundation -- kodi	Directory Traversal in Zip Extraction built-in function in Kodi 17.1 and earlier allows arbitrary file write on disk via a Zip file as subtitles.	2017-05-23	not calcu

Primary Vendor -- Product	Description	Published	CVSS Score
yodl -- yodl	Yodl before 3.07.01 has a Buffer Over-read in the queue_push function in queue/queuepush.c.	2017-05-26	not calcu
ytnef -- ytnef	The TNEFFillMapi function in lib/ytnef.c in libytnef in ytnef through 1.9.2 does not ensure a nonzero count value before a certain memory allocation, which allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted tnef file.	2017-05-22	not calcu
zabbix -- zabbix_server	An exploitable code execution vulnerability exists in the trapper command functionality of Zabbix Server 2.4.X. A specially crafted set of packets can cause a command injection resulting in remote code execution. An attacker can make requests from an active Zabbix Proxy to trigger this vulnerability.	2017-05-24	not calcu
zlib -- zlib	The crc32_big function in crc32.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact via vectors involving big-endian CRC calculation.	2017-05-23	not calcu
zlib -- zlib	inffast.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact by leveraging improper pointer arithmetic.	2017-05-23	not calcu

Primary Vendor -- Product	Description	Published	CVSS Sco
zlib -- zlib	inftrees.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact by leveraging improper pointer arithmetic.	2017-05-23	not calcu
zlib -- zlib	The inflateMark function in inflate.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact via vectors involving left shifts of negative integers.	2017-05-23	not calcu

Back to top