Vulnerability Summary for the Week of April 22, 2017

Please Note:

• The vulnerabilities are categorized by their level of severity which is either High, Medium or Low.

• The CVE identity number is the publicly known ID given to that particular vulnerability. Therefore, you can search the status of that particular vulnerability using that ID.

• The CVSS (Common Vulnerability Scoring System) score is a standard scoring system used to determine the severity of the vulnerability.

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(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external)
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(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external)
apple -- mac_os_x	An issue was discovered in certain Apple products. macOS before 10.12.5 is affected. The issue	2017-05-22	9.3	CVE-2017-2494 CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	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.			
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(link is external)
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

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 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
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

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
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

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
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(link is external) CONFIRM(link is external)
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(link is external)
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	2017-05-21	7.5	CVE-2017-9117 MISC BID(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	heap-based buffer over-read in bmp2tiff.			
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(link is external)
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(link is external)
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-	2017-05-21	7.8	CVE-2017-9136 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	shared key (PSK) for encrypted wireless connections, or to view the device's serial number (which allows an attacker to factory reset the device).			

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 $_POST['captcha'].	2017-05-19	5.0	CVE-2017-9090 CONFIRM(link is external)
allendisk_project -- allendisk	/admin/loginc.php in Allen Disk 1.6 doesn't check if isset($_SESSION['captcha']['code']) == 1, which leads to CAPTCHA bypass by emptying $_POST['captcha'].	2017-05-19	5.0	CVE-2017-9091 CONFIRM(link is external)
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(link is external) CONFIRM(link is external)
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(link is external) CONFIRM(link is external)
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.	2017-05-22	5.8	CVE-2017-2497 CONFIRM(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	It allows remote attackers to trigger visits to arbitrary URLs via a crafted book.			CONFIRM(link is external)
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(link is external) CONFIRM(link is external)
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(link is external) CONFIRM(link is external) CONFIRM(link is external)
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(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external) CONFIRM(link is external)
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(link is external) CONFIRM(link is external) CONFIRM(link is external)
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	2017-05-22	6.8	CVE-2017-2505 CONFIRM(link is external) CONFIRM(lin

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.			k is external) CONFIRM(link is external)
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(link is external) CONFIRM(link is external)
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(link is external) CONFIRM(link is external)
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(link is external) CONFIRM(link is external) CONFIRM(link is external)
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(link is external)
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	2017-05-23	5.0	CVE-2017-9155 MISC

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	to the input_pnm_reader function in input-pnm.c:243:3.			
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(link is external)
google -- android	Integer overflow in soundtrigger/ISoundTriggerHwService.c	2017-05-23	5.0	CVE-2015-1529

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	pp in Android allows attacks to cause a denial of service via unspecified vectors.			BID(link is external) CONFIRM(link is external) MISC(link is external)
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(link is external) CONFIRM(link is external) CONFIRM(link is external)
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(link is external) CONFIRM(link is external)
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(link is external) CONFIRM(link is external)
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(link is external) CONFIRM(link is external)
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(link is external)
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(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
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(link is external)
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(link is external)
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(link is external)
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	2017-05-21	5.0	CVE-2017-9134 MISC(link is external)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	because there is another page (accessible without any authentication) that allows you to remotely factory reset the device simply by entering the serial number.			

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(link is external)
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(link is external) BID(link is external)