PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Red Hat OpenShift Enterprise 3.7 File System Read and Write	Red Hat OpenShift Enterprise version 3.7 is vulnerable to access control override for container network filesystems. An attacker could override the UserId and GroupId for GlusterFS and NFS to read and write any data on the network filesystem.	Version(s): <= 3.7	Published - March 09, 2018 CVE-2018-1069 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1069 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1069 https://bugzilla.redhat.com/show_bug.cgi?id=1552987
FreeBSD DoS or Other Impact due to an Issue in the Kernel	In FreeBSD before 11.1-STABLE, 11.1-RELEASE-p7, 10.4-STABLE, 10.4-RELEASE-p7, and 10.3-RELEASE-p28, the kernel does not properly validate IPsec packets coming from a trusted host. Additionally, a use-after-free vulnerability exists in the IPsec AH handling code. This issue could cause a system crash or other unpredictable results.	Version(s): <= 11.1-STABLE, 11.1-RELEASE-p7, 10.4-STABLE, 10.4-RELEASE-p7, and 10.3-RELEASE-p28	Published - March 09, 2018 CVE-2018-6916 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6916 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-6916 https://www.freebsd.org/security/advisories/FreeBSD-SA-18:01.ipsec.asc
MikroTik RouterOS 6.38.4 and Earlier Remote Code Execution Vulnerability (Chimay Red)	MikroTik RouterOS 6.38.4 and earlier is prone to a remote code execution vulnerability used in Chimay Red exploit	Version(s): <= 6.38.4	Published - March 12, 2018 SBV-82800 CVSS - 9.8 Vendor's Advisory - https://github.com/BigNerd95/Chimay-Red/blob/master/docs/ChimayRed.pdf https://www.exploit-db.com/exploits/44284/ https://github.com/BigNerd95/Chimay-Red/blob/master/README.md
SecurEnvoy SecurMail 9.1.501 Remote Missing Authentication Vulnerability - CVE-2018-7702	SecurEnvoy SecurMail 9.1.501 is vulnerable to a remote attacker downloading or sending arbitrary emails from the affected system without authentication	Version(s): = 9.1.501	Published - March 14, 2018 CVE-2018-7702 CVSS - 9.3 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7702 https://www.securenvoy.com/products/securmail/key-features.shtm https://www.sec-consult.com/en/blog/advisories/multiple-critical-vulnerabilities-in-securenvoy-securmail/index.html
SecurEnvoy SecurMail 9.1.501 CSRF Vulnerability - CVE-2018-7701	SecurEnvoy SecurMail 9.1.501 is vulnerable to cross-site request forgery via HTTP request.	Version(s): <= 9.1.501	Published - March 14, 2018 CVE-2018-7701 CVSS - 9.6 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7701 https://www.securenvoy.com/products/securmail/key-features.shtm https://www.sec-consult.com/en/blog/advisories/multiple-critical-vulnerabilities-in-securenvoy-securmail/index.html
SQLite 3.7.10 - 3.22.0 Null Pointer Dereference Vulnerability - CVE-2018-8740	In SQLite 3.7.10 through 3.22.0, databases whose schema is corrupted using a CREATE TABLE AS statement could cause a NULL pointer dereference, related to build.c and prepare.c.	Version(s): <= 3.7.10-3.22.0	Published - March 17, 2018 CVE-2018-8740 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8740 https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=6964 https://www.sqlite.org/cgi/src/timeline?r=corrupt-schema
Calibre 3.18 Remote Code Execution via Crafted .pickle File - CVE-2018-7889	gui2/viewer/bookmarkmanager.py in Calibre 3.18 calls cPickle.load on imported bookmark data, which allows remote attackers to execute arbitrary code via a crafted .pickle file, as demonstrated by Python code that contains an os.system call.	Version(s): <= 3.18	Published - March 08, 2018 CVE-2018-7889 CVSS - 8.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7889 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-7889 https://bugs.launchpad.net/calibre/+bug/1753870
Mozilla Firefox <59 , Firefox ESR <52.7 Out-of-bounds Write Vulnerability with Malformed IPC Messages- CVE-2018-5129	Mozilla Firefox before 59, and Firefox ESR before 52.7, are prone to a remote unspecified vulnerability via malformed IPC messages. This could result in sandbox escape through memory corruption in the parent process.	Version(s): <= 59, 52.7 ESR	Published - March 13, 2018 CVE-2018-5129 CVSS - 8.8 Vendor's Advisory - http://www.securityfocus.com/bid/103388 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5129 https://www.mozilla.org/en-US/security/advisories/mfsa2018-06/
[APSB18-06] Adobe Connect <=9.7 on Windows Remote File System Delete or DoS - CVE-2018-4923	Adobe Connect 9.7 and earlier on Windows allows a remote attacker to delete arbitrary files or cause a denial of service due to a flaw in the URI handler.	Version(s): <= 9.7	Published - March 13, 2018 CVE-2018-4923 CVSS - 8.1 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-4923 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-4923 https://helpx.adobe.com/security/products/connect/apsb18-06.html
PluginUs.Net WooCommerce Product Filter <2.2.0 WordPress Plugin Remote Code Execution Vulnerability - CVE-2018-8710	A remote code execution issue was discovered in the PluginUs.Net WooCommerce Products Filter (aka WOOF) plugin before 2.2.0 for WordPress, as demonstrated by the shortcode parameter in a woof_redraw_woof action. The plugin implemented a page redraw AJAX function accessible to anyone without any authentication. WordPress shortcode markup in the "shortcode" parameters would be evaluated. Normally unauthenticated users can't evaluate shortcodes as they are often sensitive.	Version(s): <= 2.2.0	Published - March 14, 2018 CVE-2018-8710 CVSS - 7.3 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-8710 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8710 https://sec-consult.com/en/blog/advisories/arbitrary-shortcode-execution-local-file-inclusion-in-woof-pluginus-net/index.html
Curl 7.20.0 - 7.58.0 Remote DoS or Information Disclosure Vulnerability in RSTP+RTP Handling - CVE-2018-1000122	A buffer over-read exists in curl 7.20.0 to and including curl 7.58.0 in the RTSP+RTP handling code that allows an attacker to cause a denial of service or information leakage	Version(s): <= 7.20.0-7.58.0	Published - March 14, 2018 CVE-2018-1000122 CVSS - 8.2 Vendor's Advisory - http://www.securityfocus.com/bid/103436 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1000122 https://curl.haxx.se/docs/adv_2018-b047.html