PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
CloudBees Jenkins Agiletestware Pangolin Connector for TestRail Plugin <=2.1 Remote CSRF Vulnerability - CVE-2018-1999032	A data modification vulnerability exists in Jenkins Agiletestware Pangolin Connector for TestRail Plugin 2.1 and earlier in GlobalConfig.java that allows attackers with Overall/Read permission to override this plugin's configuration by sending crafted HTTP requests to an unprotected endpoint	Version(s): <= 2.1	Published - July 30, 2018 CVE-2018-1999032 CVSS - 9.6 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1999032 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1999032 https://jenkins.io/security/advisory/2018-07-30/#SECURITY-1022
CloudBees Jenkins Maven Plugin <=1.3.1 Remote CSRF Vulnerability - CVE-2018-1999030	An exposure of sensitive information vulnerability exists in Jenkins Maven Artifact ChoiceListProvider (Nexus) Plugin 1.3.1 and earlier in ArtifactoryChoiceListProvider.java, NexusChoiceListProvider.java, Nexus3ChoiceListProvider.java that allows attackers to capture credentials with a known credentials ID stored in Jenkins.	Version(s): <= 1.3.1	Published - July 30, 2018 CVE-2017-1999030 CVSS - 9.6 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1999030 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1999030 https://jenkins.io/security/advisory/2018-07-30/SECURITY-1022
HP Ink Printers Remote Code Execution Vulnerability - CVE-2018-5925	Multiple HP ink printers are prone to a remote code execution vulnerability. A remote attacker could exploit this issue by sending a maliciously crafted file to an affected device, which could cause a stack or static buffer overflow. Vulnerable products are: Pagewide Pro, DesignJet, HP Officejet, HP Deskjet and HP Envy.	Version(s): <= Pagewide Pro, DesignJet, HP Officejet, HP Deskjet and HP Envy.	Published - August 01, 2018 CVE-2018-5925 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5925 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-5925 https://support.hp.com/us-en/document/c06097712 https://www.theregister.co.uk/2018/08/03/hp_printer_malware/
Jenkins Kubernetes Plugin CSRF Vulnerability - CVE-2018-1999040	An exposure of sensitive information vulnerability exists in Jenkins Kubernetes Plugin 1.10.1 and earlier in KubernetesCloud.java that allows attackers to capture credentials with a known credentials ID stored in Jenkins.	Version(s): <= 1.10.1	Published - August 01, 2018 CVE-2018-1999040 CVSS - 9.6 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1999040 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1999040 https://jenkins.io/security/advisory/2018-07-30/SECURITY-1016
CloudBees Jenkins Publisher Over CIFS Plugin <=0.10 Remote Unspecified Vulnerability - CVE-2018-1999038	A confused deputy vulnerability exists in Jenkins Publisher Over CIFS Plugin 0.10 and earlier in CifsPublisherPluginDescriptor.java that allows attackers to have Jenkins connect to an attacker specified CIFS server with attacker specified credentials.	Version(s): <= 0.10	Published - August 01, 2018 CVE-2018-1999038 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1999038 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1999038 https://jenkins.io/security/advisory/2018-07-30/
FreeBSD <=6.0.5 Remote DoS or Other Vulnerability - CVE-2018-14939	The get_app_path function in desktop/unx/source/start.c in LibreOffice through 6.0.5 mishandles the realpath function in certain environments such as FreeBSD libc, which might allow attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact if LibreOffice is automatically launched during web browsing with pathnames controlled by a remote web site.	Version(s): <= 6.0.5	Published - August 05, 2018 CVE-2018-14939 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14939 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-14939 https://bugs.documentfoundation.org/show_bug.cgi?id=118514
Linux Kernel Local Escalation of Privileges Vulnerability - CVE-2018-10901	A flaw was found in Linux kernel's KVM virtualization subsystem. The VMX code does not restore the GDT.LIMIT to the previous host value, but instead sets it to 64KB. With a corrupted GDT limit a host's userspace code has an ability to place malicious entries in the GDT, particularly to the per-cpu variables. An attacker can use this to escalate their privileges.	Version(s): <= *	Published - July 26, 2018 CVE-2018-10901 CVSS - 8.4 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10901 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-10901 https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-10901
Linux Kernel Remote DoS Vulnerability - CVE-2018-14734	drivers/infiniband/core/ucma.c in the Linux kernel through 4.17.11 allows ucma_leave_multicast to access a certain data structure after a cleanup step in ucma_process_join, which allows attackers to cause a denial of service (use-after-free).	Version(s): <= 4.17.11	Published - July 29, 2018 CVE-2018-14734 CVSS - 7.5 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14734 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-14734 https://github.com/torvalds/linux/commit/cb2595c1393b4a5211534e6f0a0fbad369e21ad8
F5 BigIP and Google Kubernetes Local Passwords Disclosure Vulnerability - CVE-2018-5543	The F5 BIG-IP Controller for Kubernetes 1.0.0-1.5.0 (k8s-bigip-crtl) passes BIG-IP username and password as command line parameters, which may lead to disclosure of the credentials used by the container.	Version(s): <= 1.0.0 - 1.5.0	Published - July 31, 2018 CVE-2018-5543 CVSS - 6.5 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5543 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-5543 https://support.f5.com/csp/article/K58935003
PHP 7 - 7.1.5 Remote DoS Vulnerability due to Integer Overflow - CVE-2017-9120	PHP 7.x through 7.1.5 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a long string because of an Integer overflow in mysqli_real_escape_string.	Version(s): <= 7 - 7.1.5	Published - August 02, 2018 CVE-2017-9120 CVSS - 8.6 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9120 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-9120 https://bugs.php.net/bug.php?id=74544