

PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Google Android Remote Code Execution Vulnerability in Library - CVE-2018-9472	Google Android 7.0, 7.1.1, 7.1.2, 8.0 and 8.1 before 2018-09-01 are prone to a high severity remote code execution vulnerability in the Library component. AKA Android Bug ID 79662501.	Version(s): = 7.1.1, 7.1.2, 7.0, 8.0, 8.1	Published - Sep 04, 2018 CVE- 2018-9472 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9472 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-9472
Linux Kernel <4.17 Local DoS or Other Unspecified Impact - CVE-2018-6555	The <code>irda_setsockopt</code> function in <code>net/irda/af_irda.c</code> and later in <code>drivers/staging/irda/net/af_irda.c</code> in the Linux kernel before 4.17 allows local users to cause a denial of service (ias_object use-after-free and system crash) or possibly have unspecified other impact via an <code>AF_IRDA</code> socket.	Version(s): < 4.17	Published - Sep 04, 2018 CVE-2018-6555 CVSS - 7.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6555 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-6555
ImageMagick Remote Unspecified Vulnerability - CVE-2018-16329	In ImageMagick before 7.0.8-8, a NULL pointer dereference exists in the <code>GetMagickProperty</code> function in <code>MagickCore/property.c</code> .	Version(s): < Check Point Security Gateway R80.10 running Gaia OS	Published - Sep 04, 2018 SBV-89942 CVSS - 9.8 Vendor's Advisory - https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_id=GoViewsolutiondetails=&solutionid=sk134054
IBM WebSphere Application Server Spoofing Vulnerability - CVE-2018-1695	Calling IBM WebSphere Application Server Form Login using Java SE 6 makes the server vulnerable to spoofing attack. This weakness is observed in WebSphere Application Server versions 8.5.5, 8.0 and 7.0.	Version(s): = 7.0, 8.0, 8.5.5	Published - Sep 04, 2018 CVE-2018-1695 CVSS - 7.3 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1695 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1695
Check Point Security Gateway R80.10 Identity Awareness Incorrect Policy Actions Vulnerability	Check Point Security Gateway R80.10 running Gaia OS, is prone to a vulnerability that could result in incorrect policy actions in Identity Awareness due to a rare failure in the Identity Sharing network registration.	Version(s): < 3.3.14.1	Published - Sep 02, 2018 CVE-2018-16308 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-16308 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-16308
Mozilla Firefox Remote Memory Safety Resulting in Code Execution - CVE-2018-12376	Mozilla Firefox release 61 and ESR release 60.1 are prone to a memory safety issue that could be leveraged to arbitrary code execution.	Version(s): 60.1 ESR, 61 Release	Published - Sep 05, 2018 CVE-2018-12376 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12376 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-12376
ImageMagick Remote Unspecified Vulnerability - CVE-2018-16329	In ImageMagick before 7.0.8-8, a NULL pointer dereference exists in the <code>GetMagickProperty</code> function in <code>MagickCore/property.c</code> .	Version(s): < 7.0.8-8	Published - Sep 02, 2018 CVE-2018-16328 CVSS - 9.8 Vendor's Advisory - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-16329 https://github.com/ImageMagick/ImageMagick/issues/1225
cisco-sa-20180905-rv-routers-overflow] Cisco RV Routers Remote DoS and Code Execution Vulnerability - CVE-2018-0423	Cisco RV110W Wireless-N VPN Firewall, Cisco RV130W Wireless-N Multifunction VPN Router running firmware before release 1.0.3.44, and Cisco RV215W Wireless-N VPN router are prone to a denial-of-service and remote code execution vulnerability due to inadequate boundary restrictions on input passed in the Guest user feature of the web-based management interface. Note: Cisco RV110W Wireless-N VPN Firewall and Cisco RV215W Wireless-N VPN will not be patched.	Version(s): < 1.0.3.44	Published - Sep 05, 2018 CVE-2018-0423 CVSS - 9.8 Vendor's Advisory http://www.securityfocus.com/bid/105285 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0423
IBM WebSphere Application Server Remote Code Execution Vulnerability - CVE-2018-1567	IBM WebSphere Application Server is prone to remote Java code execution through the SOAP connector via objects from untrusted sources.	Version(s): <= 7.0.8	Published - Sep 05, 2018 CVE-2018-1567 CVSS - 9.8 Vendor's Advisory - http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1567 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1567
VMware Content Locker for iOS Remote Information Disclosure Vulnerability - CVE-2018-6976	VMware Content Locker for iOS is prone to remote information disclosure vulnerability due to weakness in SQLite database associated with unencrypted filenames.	Version(s): < 4.14	Published - Sep 04, 2018 CVE-2018-6976 CVSS - 5.3 Vendor's Advisory - VMware Content Locker for iOS is prone to remote information disclosure vulnerability due to weakness in SQLite database associated with unencrypted filenames.