



CVE-2018-5391

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2018-5391
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-09-06 21:29:00 UTC
Updated	2023-11-07 02:58:00 UTC
Description	The Linux kernel, versions 3.9+, is vulnerable to a denial of service attack with low rates of specially modified packets target

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	F5	Big-ip Access Policy Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Analytics	All	All	All	All
Application	F5	Big-ip Application Acceleration Manager	All	All	All	All
Application	F5	Big-ip Application Security Manager	All	All	All	All

Application	F5	Big-ip Domain Name System	All	All	All	All
Application	F5	Big-ip Edge Gateway	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	All	All	All	All
Application	F5	Big-ip Link Controller	All	All	All	All
Application	F5	Big-ip Local Traffic Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Webaccelerator	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 10	1607	All	All	All
Operating System	Microsoft	Windows 10	1703	All	All	All
Operating System	Microsoft	Windows 10	1709	All	All	All
Operating System	Microsoft	Windows 10	1803	All	All	All
Operating System	Microsoft	Windows 7	-	sp1	All	All
Operating System	Microsoft	Windows 8.1	-	All	All	All
Operating System	Microsoft	Windows Rt 8.1	-	All	All	All
Operating System	Microsoft	Windows Server 2008	-	sp2	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2008	r2	sp1	All	All
Operating System	Microsoft	Windows Server 2012	-	All	All	All
Operating System	Microsoft	Windows Server 2012	r2	All	All	All
Operating System	Microsoft	Windows Server 2016	-	All	All	All
Operating System	Microsoft	Windows Server 2016	1709	All	All	All
Operating System	Microsoft	Windows Server 2016	1803	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.5	All	All	All

Operating System	Redhat	Enterprise Linux Server Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Hardware	Siemens	Ruggedcom Rm1224	-	All	All	All
Operating System	Siemens	Ruggedcom Rm1224 Firmware	All	All	All	All
Hardware	Siemens	Ruggedcom Rox li	-	All	All	All
Operating System	Siemens	Ruggedcom Rox li Firmware	All	All	All	All
Hardware	Siemens	Scalance M-800	-	All	All	All
Operating System	Siemens	Scalance M-800 Firmware	All	All	All	All

Operating System	Siemens	Scalance M-800 Firmware	All	All	All	All
Hardware	Siemens	Scalance S615	-	All	All	All
Operating System	Siemens	Scalance S615 Firmware	All	All	All	All
Hardware	Siemens	Scalance Sc-600	-	All	All	All
Operating System	Siemens	Scalance Sc-600 Firmware	All	All	All	All
Hardware	Siemens	Scalance W1700 Ieee 802.11ac	-	All	All	All
Operating System	Siemens	Scalance W1700 Ieee 802.11ac Firmware	All	All	All	All
Hardware	Siemens	Scalance W700 Ieee 802.11a/b/g/n	-	All	All	All
Operating System	Siemens	Scalance W700 Ieee 802.11a/b/g/n Firmware	All	All	All	All
Hardware	Siemens	Simatic Net Cp 1242-7	-	All	All	All
Operating System	Siemens	Simatic Net Cp 1242-7 Firmware	All	All	All	All
Hardware	Siemens	Simatic Net Cp 1243-1	-	All	All	All
Operating System	Siemens	Simatic Net Cp 1243-1 Firmware	All	All	All	All
Hardware	Siemens	Simatic Net Cp 1243-7 Lte Eu	-	All	All	All
Operating System	Siemens	Simatic Net Cp 1243-7 Lte Eu Firmware	All	All	All	All
Hardware	Siemens	Simatic Net Cp 1243-7 Lte Us	-	All	All	All
Operating System	Siemens	Simatic Net Cp 1243-7 Lte Us Firmware	All	All	All	All
Hardware	Siemens	Simatic Net Cp 1243-8 Irc	-	All	All	All
Operating System	Siemens	Simatic Net Cp 1243-8 Irc Firmware	All	All	All	All
Hardware	Siemens	Simatic Net Cp 1542sp-1	-	All	All	All
Operating System	Siemens	Simatic Net Cp 1542sp-1 Firmware	All	All	All	All
Hardware	Siemens	Simatic Net Cp 1542sp-1 Irc	-	All	All	All
Operating System	Siemens	Simatic Net Cp 1542sp-1 Irc Firmware	All	All	All	All
Hardware	Siemens	Simatic Net Cp 1543-1	-	All	All	All
Operating System	Siemens	Simatic Net Cp 1543-1 Firmware	All	All	All	All
Hardware	Siemens	Simatic Net Cp 1543sp-1	-	All	All	All
Operating System	Siemens	Simatic Net Cp 1543sp-1 Firmware	All	All	All	All
Hardware	Siemens	Simatic Rf185c	-	All	All	All
Operating System	Siemens	Simatic Rf185c Firmware	All	All	All	All
Hardware	Siemens	Simatic Rf186c	-	All	All	All
Hardware	Siemens	Simatic Rf186ci	-	All	All	All
Operating System	Siemens	Simatic Rf186ci Firmware	All	All	All	All
Operating System	Siemens	Simatic Rf186c Firmware	All	All	All	All
Hardware	Siemens	Simatic Rf188	-	All	All	All
Hardware	Siemens	Simatic Rf188ci	-	All	All	All
Operating System	Siemens	Simatic Rf188ci Firmware	All	All	All	All

Operating System	Siemens	Simatic Rf188 Firmware	All	All	All	All
Hardware	Siemens	Sinema Remote Connect Server	-	All	All	All
Operating System	Siemens	Sinema Remote Connect Server Firmware	All	All	All	All

References

Reference

Linux Kernel IP Fragment Reassembly Algorithm Lets Remote Users Consume Excessive CPU Resources on the Target System - SecurityTr

[SECURITY] [DLA 1466-1] linux-4.9 security update

Red Hat Customer Portal

Red Hat Customer Portal

Debian -- Security Information -- DSA-4272-1 linux

www.arubanetworks.com/assets/alert/ARUBA-PSA-2018-004.txt

Red Hat Customer Portal

[SECURITY] [DLA 1715-1] linux-4.9 security update

CVE-2018-5391 Linux Kernel Denial of Service Vulnerability in NetApp Products | NetApp Product Security

Windows IP Fragment Reassembly Algorithm Lets Remote Users Consume Excessive CPU Resources on the Target System - SecurityTrack

Red Hat Customer Portal

USN-3740-2: Linux kernel (HWE) vulnerabilities | Ubuntu security notices

Red Hat Customer Portal

USN-3742-1: Linux kernel vulnerabilities | Ubuntu security notices

Red Hat Customer Portal

myF5

USN-3742-2: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu security notices

Red Hat Customer Portal

kernel/git/davem/net-next.git - David Miller's -next networking tree

Red Hat Customer Portal

USN-3740-1: Linux kernel vulnerabilities | Ubuntu security notices

USN-3741-2: Linux kernel (Xenial HWE) vulnerabilities | Ubuntu security notices

oss-security - Re: linux-distros membership application - Microsoft

cert-portal.siemens.com/productcert/pdf/ssa-377115.pdf

CERT Vulnerability Notes Database

oss-security - Re: linux-distros membership application - Microsoft

Red Hat Customer Portal

USN-3741-1: Linux kernel vulnerabilities | Ubuntu security notices

Red Hat Customer Portal

Linux Kernel CVE-2018-5201 Remote Denial of Service Vulnerability

Linux kernel CVE-2018-5391 Remote Denial of Service vulnerability

Huawei - Building a Fully Connected, Intelligent World

oss-security - Re: linux-distros membership application - Microsoft

Red Hat Customer Portal

support.f5.com/csp/article/K74374841

Red Hat Customer Portal

Red Hat Customer Portal

CVE Program record

NVD vulnerability detail



Vendor Comments And Credit

Discovery Credit

LEGACY: Thanks to Juha-Matti Tilli (Aalto University, Department of Communications and Networking / Nokia Bell Labs) for reporting this vulnerability.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)