



CVE-2019-11477

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

Summary

CVE	CVE-2019-11477
State	PUBLIC
Assigner	security@ubuntu.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-06-19 00:15:00 UTC
Updated	2023-08-16 14:17:00 UTC
Description	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Li

Risk And Classification

Problem Types: CWE-190

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	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	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	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	19.04	All	All	All
Application	F5	Big-ip Access Policy Manager	15.0.0	All	All	All
Application	F5	Big-ip Access Policy Manager	15.0.0	All	All	All
Application	F5	Big-ip Access Policy Manager	All	All	All	All
Application	F5	Big-ip Access Policy Manager	All	All	All	All
Application	F5	Big-ip Access Policy Manager	All	All	All	All

Application	F5	Big-ip Access Policy Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	15.0.0	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	15.0.0	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Advanced Firewall Manager	All	All	All	All
Application	F5	Big-ip Analytics	15.0.0	All	All	All
Application	F5	Big-ip Analytics	15.0.0	All	All	All
Application	F5	Big-ip Analytics	All	All	All	All
Application	F5	Big-ip Analytics	All	All	All	All
Application	F5	Big-ip Analytics	All	All	All	All
Application	F5	Big-ip Analytics	All	All	All	All
Application	F5	Big-ip Application Acceleration Manager	15.0.0	All	All	All
Application	F5	Big-ip Application Acceleration Manager	15.0.0	All	All	All
Application	F5	Big-ip Application Acceleration Manager	All	All	All	All
Application	F5	Big-ip Application Acceleration Manager	All	All	All	All
Application	F5	Big-ip Application Acceleration Manager	All	All	All	All
Application	F5	Big-ip Application Acceleration Manager	All	All	All	All
Application	F5	Big-ip Application Security Manager	15.0.0	All	All	All
Application	F5	Big-ip Application Security Manager	15.0.0	All	All	All
Application	F5	Big-ip Application Security Manager	All	All	All	All
Application	F5	Big-ip Application Security Manager	All	All	All	All
Application	F5	Big-ip Application Security Manager	All	All	All	All
Application	F5	Big-ip Application Security Manager	All	All	All	All
Application	F5	Big-ip Domain Name System	15.0.0	All	All	All
Application	F5	Big-ip Domain Name System	15.0.0	All	All	All
Application	F5	Big-ip Domain Name System	All	All	All	All
Application	F5	Big-ip Domain Name System	All	All	All	All
Application	F5	Big-ip Domain Name System	All	All	All	All
Application	F5	Big-ip Domain Name System	All	All	All	All
Application	F5	Big-ip Edge Gateway	15.0.0	All	All	All
Application	F5	Big-ip Edge Gateway	15.0.0	All	All	All
Application	F5	Big-ip Edge Gateway	All	All	All	All
Application	F5	Big-ip Edge Gateway	All	All	All	All

Application	F5	Big-ip Edge Gateway	All	All	All	All
Application	F5	Big-ip Edge Gateway	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	15.0.0	All	All	All
Application	F5	Big-ip Fraud Protection Service	15.0.0	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Fraud Protection Service	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	15.0.0	All	All	All
Application	F5	Big-ip Global Traffic Manager	15.0.0	All	All	All
Application	F5	Big-ip Global Traffic Manager	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	All	All	All	All
Application	F5	Big-ip Global Traffic Manager	All	All	All	All
Application	F5	Big-ip Link Controller	15.0.0	All	All	All
Application	F5	Big-ip Link Controller	15.0.0	All	All	All
Application	F5	Big-ip Link Controller	All	All	All	All
Application	F5	Big-ip Link Controller	All	All	All	All
Application	F5	Big-ip Link Controller	All	All	All	All
Application	F5	Big-ip Link Controller	All	All	All	All
Application	F5	Big-ip Local Traffic Manager	15.0.0	All	All	All
Application	F5	Big-ip Local Traffic Manager	15.0.0	All	All	All
Application	F5	Big-ip Local Traffic Manager	All	All	All	All
Application	F5	Big-ip Local Traffic Manager	All	All	All	All
Application	F5	Big-ip Local Traffic Manager	All	All	All	All
Application	F5	Big-ip Local Traffic Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	15.0.0	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	15.0.0	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Policy Enforcement Manager	All	All	All	All
Application	F5	Big-ip Webaccelerator	15.0.0	All	All	All
Application	F5	Big-ip Webaccelerator	15.0.0	All	All	All
Application	F5	Big-ip Webaccelerator	All	All	All	All

Application	F5	Big-ip Webaccelerator	All	All	All	All
Application	F5	Big-ip Webaccelerator	All	All	All	All
Application	F5	Big-ip Webaccelerator	All	All	All	All
Application	F5	Traffix Sdc	All	All	All	All
Application	F5	Traffix Signaling Delivery Controller	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Application	Pulsesecure	Pulse Connect Secure	-	All	All	All
Application	Pulsesecure	Pulse Connect Secure	-	All	All	All
Application	Pulsesecure	Pulse Policy Secure	-	All	All	All
Application	Pulsesecure	Pulse Policy Secure	-	All	All	All
Application	Pulsesecure	Pulse Secure Virtual Application Delivery Controller	-	All	All	All
Application	Pulsesecure	Pulse Secure Virtual Application Delivery Controller	-	All	All	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Application	Redhat	Enterprise Linux Atomic Host	-	All	All	All
Application	Redhat	Enterprise Linux Atomic Host	-	All	All	All
Operating System	Redhat	Enterprise Linux Aus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Aus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.5	All	All	All
Application	Redhat	Enterprise Mrg	2.0	All	All	All
Operating System	Redhat	Enterprise Mrg	2.0	All	All	All
Application	Redhat	Enterprise Mrg	2.0	All	All	All

References

Reference

[Linux Kernel TCP SACK Panic Vulnerabilities in NetApp Products | NetApp Product Security](#)

[kernel/git/netdev/net.git - Netdev Group's networking tree](#)

[oss-security - Re: Membership application for linux-distros - VMware](#)

[Public KB - SA44193 - 2019-06: Out-of-Cycle Advisory: Multiple Linux Kernel and FreeBSD vulnerabilities](#)

[Siemens Industrial Products \(Update G\) | CISA](#)

[www.arubanetworks.com/assets/alert/ARUBA-PSA-2020-010.txt](#)

[Oracle Critical Patch Update Advisory - October 2020](#)

[Red Hat Customer Portal](#)

[cert-portal.siemens.com/productcert/pdf/ssa-462066.pdf](#)

[TCP SACK PANIC - Kernel vulnerabilities - CVE-2019-11477, CVE-2019-11478 & CVE-2019-11479 - Red Hat Customer Portal](#)

[oss-security - Re: Linux and FreeBSD Kernel: Multiple TCP-based remote denial of service issues](#)

[oss-security - Re: linux-distros membership application - Microsoft](#)

[Red Hat Customer Portal](#)

[oss-security - Re: linux-distros membership application - Microsoft](#)

[Security Advisory](#)

[Security Advisory - Integer Overflow Vulnerability in the Linux Kernel \(SACK Panic\)](#)

[Synology Inc.](#)

[support.f5.com/csp/article/K78234183](#)

[McAfee Security Bulletin – Updates for Linux kernel TCP Sad SACK vulnerability \(CVE-2019-11477, CVE-2019-11478, CVE-2019-11479\)](#)

[Kernel Live Patch Security Notice LSN-0058-1 ≈ Packet Storm](#)

[VMSA-2019-0010.1](#)

[VU#905115 - Multiple TCP Selective Acknowledgement \(SACK\) and Maximum Segment Size \(MSS\) networking vulnerabilities may cause den](#)

[Oracle Critical Patch Update Advisory - January 2020](#)

[SecurityTeam/KnowledgeBase/SACKPanic - Ubuntu Wiki](#)

[oss-security - Re: linux-distros membership application - Microsoft](#)

[Red Hat Customer Portal](#)

[oss-security - Membership application for linux-distros - VMware](#)

[Kernel Live Patch Security Notice LSN-0052-1 ≈ Packet Storm](#)

[security-bulletins/2019-001.md at master · Netflix/security-bulletins · GitHub](#)

[CVE Program record](#)

[NVD vulnerability detail](#)



Vendor Comments And Credit

Discovery Credit

LEGACY: Jonathan Looney from Netflix

Legacy QID Mappings

610318 Google Android February 2021 Security Patch Missing for Huawei EMUI

© [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](#)