CVE-2019-11479

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-11479
State	PUBLIC
Assigner	security@ubuntu.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-06-19 00:15:00 UTC
Updated	2023-11-07 03:03:00 UTC
Description	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to frag

Risk And Classification

Problem Types: CWE-770

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	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	All	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 Advanced Firewall Manager	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	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 Application Security Manager	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	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 Fraud Protection Service	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	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 Local Traffic 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	All	All	All	All
Application	F5	Big-ip Webaccelerator	All	All	All	All
Application	F5	Big-iq Centralized Management	All	All	All	All
Application	F5	Big-iq Centralized Management	All	All	All	All
Application	F5	Enterprise Manager	3.1.1	All	All	All
Application	F5	Enterprise Manager	3.1.1	All	All	All
Application	F5	Iworkflow	2.3.0	All	All	All
Application	F5	Iworkflow	2.3.0	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
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Application	Redhat	Virtualization Host	4.0	All	All	All
Application	Redhat	Virtualization Host	4.0	All	All	All

References

Reference
Linux Kernel TCP SACK Panic Vulnerabilities in NetApp Products | NetApp Product Security
Security Advisory
Public KB - SA44193 - 2019-06: Out-of-Cycle Advisory: Multiple Linux Kernel and FreeBSD vulnerabilities
Linux Kernel CVE-2019-11479 Denial of Service Vulnerability
Siemens Industrial Products (Update G) | CISA
www.arubanetworks.com/assets/alert/ARUBA-PSA-2020-010.txt
BD Alaris PCU (Update A) | CISA
myF5
USN-4041-1: Linux kernel update | Ubuntu security notices
Oracle Critical Patch Update Advisory - October 2020
USN-4041-2: Linux kernel (HWE) update | Ubuntu security notices
Red Hat Customer Portal
cert-portal.siemens.com/productcert/pdf/ssa-462066.pdf
kernel/git/netdev/net.git - Netdev Group's networking tree
TCP SACK PANIC - Kernel vulnerabilities - CVE-2019-11477, CVE-2019-11478 & CVE-2019-11479 - Red Hat Customer Portal
oss-security - Re: linux-distros membership application - Microsoft
Red Hat Customer Portal
oss-security - Re: linux-distros membership application - Microsoft
support.f5.com/csp/article/K35421172
Synology Inc.
McAfee Security Bulletin – Updates for Linux kernel TCP Sad SACK vulnerability (CVE-2019-11477, CVE-2019-11478, CVE-2019-11479)
kernel/git/netdev/net.git - Netdev Group's networking tree
VU#905115 - Multiple TCP Selective Acknowledgement (SACK) and Maximum Segment Size (MSS) networking vulnerabilities may cause der
Oracle Critical Patch Update Advisory - January 2020
SecurityTeam/KnowledgeBase/SACKPanic - Ubuntu Wiki
oss-security - Re: linux-distros membership application - Microsoft
Red Hat Customer Portal
support.f5.com/csp/article/K35421172
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

377208 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2019:0038)

610318 Google Android February 2021 Security Patch Missing for Huawei EMUI