



# CVE-2019-11479

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

## Summary

<b>CVE</b>	CVE-2019-11479
<b>State</b>	PUBLIC
<b>Assigner</b>	security@ubuntu.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-06-19 00:15:00 UTC
<b>Updated</b>	2023-11-07 03:03:00 UTC
<b>Description</b>	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	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.04	All	All	All
Application	<a href="#">F5</a>	<a href="#">Big-ip Access Policy Manager</a>	All	All	All	All
Application	<a href="#">F5</a>	<a href="#">Big-ip Access Policy Manager</a>	All	All	All	All
Application	<a href="#">F5</a>	<a href="#">Big-ip Advanced Firewall Manager</a>	All	All	All	All
Application	<a href="#">F5</a>	<a href="#">Big-ip Advanced Firewall Manager</a>	All	All	All	All
Application	<a href="#">F5</a>	<a href="#">Big-ip Analytics</a>	All	All	All	All
Application	<a href="#">F5</a>	<a href="#">Big-ip Analytics</a>	All	All	All	All
Application	<a href="#">F5</a>	<a href="#">Big-ip Application Acceleration Manager</a>	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	Traffic Sdc	All	All	All	All
Application	F5	Traffic 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](http://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](http://cert-portal.siemens.com/productcert/pdf/ssa-462066.pdf)

[kernel/git/netdev/net.git](https://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](https://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](https://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 denial of service

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](https://support.f5.com/csp/article/K35421172)

[security-bulletins/2019-001.md at master · Netflix/security-bulletins · GitHub](https://github.com/Netflix/security-bulletins/blob/master/security-bulletins/2019-001.md)

CVE Program record

NVD vulnerability detail

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

© [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](#)