Security Advisory Report - OBSO-1906-01

TCP SACK PANIC -Linux Kernel vulnerabilities - CVE-2019-11477, CVE-2019-11478, CVE -2019-11479, CVE-2019-5599

Release Date: 2019-06-21 16:50:18
Last Update: 2019-08-09 11:38:03

Summary

Update:

Status affected products: OSV, OS 4K, OS Alarm Response (OSsAR)

Several related flaws were found in the Linux kernel's handling of TCP networking. The most severe vulnerability could allow a remote attacker to trigger a kernel panic in systems running the affected software and, as a result, impact the system's availability.

The issues have been assigned multiple CVEs: CVE-2019-11477 is considered as high, whereas CVE-2019-11478 and CVE-2019-11479 are considered a medium priority.

For CVE-2019-5599 we have no rating yet, but it is relevant only for FreeBSD 12 which is not used by Unify products.

CVE-2019-11477 and CVE-2019-11478 are related to the Selective Acknowledgement (SACK) packets combined with Maximum Segment Size (MSS), CVE-2019-11479 solely with the Maximum Segment Size (MSS).

These issues are corrected either through applying mitigations or kernel patches.

Risk Level: Medium to High

CVE-2019-11477: SACK Panic (Linux >= 2.6.29) This vulnerability was there since 2009.

Details

SACK:
TCP Selective Acknowledgment (SACK) is a mechanism where the data receiver can inform the sender about all the segments that have successfully been accepted. This allows the sender to retransmit segments of the stream that are missing from its 'known good' set. When TCP SACK is disabled a much larger set of retransmits are required to retransmit a complete stream.

MSS:
The maximum segment size (MSS) is a parameter set in the TCP header of a packet that specifies the total amount of data contained in a reconstructed TCP segment.
As packets might become fragmented when transmitting across different routes, a host must specify the MSS as equal to the largest IP datagram payload size that a host can handle. Very large MSS sizes might mean that a stream of packets ends up fragmented on their way to the destination, whereas smaller packets can ensure less fragmentation but end up with unused overhead.
Operating systems and transport types can default to specified MSS sizes. Attackers with privileged access can create raw packets with crafted MSS options in the packet to create this attack.

1: CVE-2019-11477: SACK Panic (Linux >= 2.6.29)

Description: A sequence of SACKs may be crafted such that one can trigger an integer overflow, leading to a kernel panic. This may cause an OS crash.

2: CVE-2019-11478: SACK Slowness (Linux < 4.15) or Excess Resource Usage (all Linux versions)

Description: It is possible to send a crafted sequence of SACKs which will fragment the TCP retransmission queue. On Linux kernels prior to 4.15, an attacker may be able to further exploit the fragmented queue to cause an expensive linked-list walk for subsequent SACKs received for that same TCP connection.This may lead to hindering the system and cause a Denial of Service.

3: CVE-2019-5599: SACK Slowness (FreeBSD 12 using the RACK TCP Stack)

Description: It is possible to send a crafted sequence of SACKs which will fragment the RACK send map. An attacker may be able to further exploit the fragmented send map to cause an expensive linked-list walk for subsequent SACKs received for that same TCP connection.

4: CVE-2019-11479: Excess Resource Consumption Due to Low MSS Values (all Linux versions)

Description: An attacker can force the Linux kernel to segment its responses into multiple TCP segments, each of which contains only 8 bytes of data. This drastically increases the bandwidth required to deliver the same amount of data. Further, it consumes additional resources (CPU and NIC processing power). This attack requires continued effort from the attacker and the impacts will end shortly after the attacker stops sending traffic.

Available Mitigations
In order to mitigate the issues, it is possible to disable the vulnerable component of Linux system. This can be done by disabling selective acknowledgments (SACK) system wide for all newly established TCP connections:
echo 0 > /proc/sys/net/ipv4/tcp_sack
or
sysctl -w net.ipv4.tcp_sack=0

Another possibility is to use iptables (which is used to configure Linux kernel firewall) to drop connections with a low MSS size:
iptables -I INPUT -p tcp --tcp-flags SYN SYN -m tcpmss --mss 1:500 -j DROP
ip6tables -I INPUT -p tcp --tcp-flags SYN SYN -m tcpmss --mss 1:500 -j DROP

iptables -nL -v
ip6tables -nL -v

Available Exploits/PoC
At the moment, no public PoC or exploit is available. However, identification of systems supporting SACK and running Linux can be achieved by checking TTL parameter and searching for “sackOK” string:
tcpdump -i eth0 -n 'ip[8]<65 and tcp[13]&0x2f=2' | grep 'sackOK'
This command will help identify systems with either the SYN or SYN-ACK flags set with a TTL of less than 65. It is possible that other tools which can facilitate finding potentially vulnerable machines or exploit code will be available in the future.

Affected Products

CVE	Operating System Affected	Description/Impact
CVE-2019-11477	Linux > 2.6.29	SACK processing integer overflow. Leads to kernel panic.
CVE-2019-11478	Linux < 4.14.127	SACK Slowness or Excess Resource Usage
CVE-2019-5599	FreeBSD	RACK Send Map SACK Slowness
CVE-2019-11479	Linux (all versions)	Excess Resource Consumption Due to Low MSS Values

https://isc.sans.edu/forums/diary/What+You+Need+To+Know+About+TCP+SACK+Panic/25046/

All products running on Linux are potentially affected, see table.

Analysis of Unify product has started.

Setting of /proc/sys/net/ipv4/tcp_sack set to 0 will be checked and corrected if needed.

Load tests will be perfomed which may take a while.

Affected Products:

All Desk Phones and OpenStage phones: patch in work.

Xpert 6010p: patch in work

OpenScape 4000 platform, patch in work
The OS4K Platform Hotfix (V8 R2.22.4 - OS4K PLT HF) addressing/mitigating the TCP SACK PANIC is now available in SWS as “eeQA - Pilot Usage”.
There will be no Hotfix for OS4K V7 R2, customers are recommended to update to V8 R2.

OSV: patch iis available for V9.0 R4.43.2 Patchsets, Status eeQA - Pilot Usage”.

Circuit meeting Room: patch in work

Circuit fixed in 1.13.126.0

Branch/ SBC Patch in work

OpenScape Alarm Response, patch in work for V4R1 for OScAR Eco/Pro planned for October 2019

Not affected products:

OpenScape 4000 CSTA

OpenScape 4000 Assistant

Recommended Actions

Patches and mitigations are available, and can be applied by hand if needed, or you can wait for a security fix to be pushed or offered to your at-risk device.

A key workaround is to set /proc/sys/net/ipv4/tcp_sack to 0.

This needs to be tested concerning network performance

Disabling SACK may impact your network throughput, especially in case of high packet loss.

Linux kernel developer and maintainer Greg Kroah-Hartman announced that patches have been rolled into the stable kernel releases for the following versions:

- 4.4.182
- 4.9.182
- 4.14.127
- 4.19.52
- 5.1.11

Other than the 3.16.y kernel branch, all other kernel branches are end-of-life, and will not be getting updates for these, or any other, bugfixes.

https://de.tenable.com/blog/sack-panic-linux-and-freebsd-kernels-vulnerable-to-remote-denial-of-service-vulnerabilities-cve?tns_redirect=true

https://www.openwall.com/lists/oss-security/2019/06/17/6

https://isc.sans.edu/forums/diary/What+You+Need+To+Know+About+TCP+SACK+Panic/25046/

Unify appliances will be fixed by Unify and patch versions will be delivered.

Servers on which Unify applications run should be fixed and tested for bandwidth issues.

References

https://access.redhat.com/security/vulnerabilities/tcpsack

https://www.theregister.co.uk/2019/06/17/linux_tcp_sack_kernel_crash/

https://github.com/Netflix/security-bulletins/blob/master/advisories/third-party/2019-001.md

https://www.google.com/amp/s/www.theregister.co.uk/AMP/2019/06/17/linux_tcp_sack_kernel_crash/

https://github.com/Netflix/security-bulletins/blob/master/advisories/third-party/2019-001.md

http://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-5599

https://seclists.org/oss-sec/2019/q2/182

https://www.openwall.com/lists/oss-security/2019/06/17/5

https://isc.sans.edu/forums/diary/What+You+Need+To+Know+About+TCP+SACK+Panic/25046/

https://de.tenable.com/blog/sack-panic-linux-and-freebsd-kernels-vulnerable-to-remote-denial-of-service-vulnerabilities-cve?tns_redirect=true

Advisory: OBSO-1906-01, status: general release
Security Advisories are released as part of Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

Contact and Disclaimer

OpenScape Baseline Security Office
obso@atos.net

Otto-Hahn-Ring 6
D-81739 München
www.unify.com