TCP/IP – SACK ATTACK VULNERABILITIES

PUBLISHED: JUNE 30, 2019 | LAST UPDATE: OCTOBER 11, 2019

SUMMARY

In June 2019, vulnerabilities were published [5] in the industry, collectively known as "SACK Attack", exposing security weaknesses in Linux and FreeBSD TCP protocol stacks, centered in their implementation of Selective ACK (SACK) and Maximum Segment Sizes (MSS) TCP Protocol features. These vulnerabilities, listed below, are addressed in this document.

A10 Networks continues to investigate and quantify any real or potential exposures for these vulnerabilities in the data planes of ACOS systems and to validate current assessments shared in this document. Additional findings of this investigation will be included in subsequent updates to this advisory.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2019-11477	CVSS 3.0	7.5 High	tcp: integer overflow while processing SACK blocks allows remote denial of service (aka SACK Panic) [1]
2	CVE-2019-11478	CVSS 3.0	5.3 Medium	tcp: excessive resource consumption while processing SACK blocks allows remote denial of service (aka SACK Slowness) [2]
3	CVE-2019-11479	CVSS 3.0	5.3 Medium	tcp: excessive resource consumption for TCP connections with low MSS allows remote denial of service [3]
4	CVE-2019-5599	CVSS 3.0	5.3 Medium	SACK Slowness (FreeBSD 12 using the RACK TCP Stack) [4]

Of these vulnerabilities, CVE-2019-5599 is not an exposure in ACOS.

The remaining vulnerabilities and their exposures in ACOS are discussed below for ACOS management and data planes.

ACOS MANAGEMENT PLANE

The management planes of all ACOS release families are exposed to these vulnerabilities as follows:

Release Family	Valid Vulnerabilities
4.1.x (ADC/CGN)	CVE-2019-11477, CVE-2019-11478, CVE-2019-11479
2.x.x (ADC/CGN)	CVE-2019-11478, CVE-2019-11479
3.2.2/later (TPS)	CVE-2019-11477, CVE-2019-11478, CVE-2019-11479
3.2.1/prior (TPS)	CVE-2019-11478, CVE-2019-11479

ACOS DATA PLANE – ADC/CGN

The data planes of all ACOS ADC/CGN release families are not exposed to CVE-2019-11477.

For various types of traffic and ACOS releases families, assessments of exposure to CVE-2019-11478 or CVE-2019-11479 are as follows:

Traffic Type	Release Family	Assessment
TCP	4.1.x, 2.x.x	Not exposed
TCP-Proxied	4.1.x, 2.x.x	Not exposed
L7 Application Proxied	4.1.x	Very likely to be not exposed [(a)]
L7 Application Proxied	2.x.x	Likely to be not exposed [(a)]

[(a)] Under continued investigation, as described above.

ACOS DATA PLANE – TPS

The data planes of all ACOS TPS release families are not exposed to CVE-2019-11477.

For various types of traffic and ACOS releases families, assessments of exposure to CVE-2019-11478 or CVE-2019-11479 are as follows:

Traffic Type	Release Family	Assessment
Asymmetric Mode	all	Not exposed
Symmetric Mode – Non-HTTP	all	Not exposed
Symmetric Mode – HTTP	3.2.2/later	Very likely to be not exposed [a]
Symmetric Mode – HTTP	3.2.1/prior	Likely to be not exposed [a]
DNS Cache Zone Updates	all	Not exposed

[a] Under continued investigation, as described above.

AFFECTED RELEASES

The table below indicates releases of ACOS exposed to these vulnerabilities and ACOS releases that address them. ACOS release families not indicated below are unaffected by these vulnerabilities.

Customers using affected ACOS releases can overcome vulnerability exposures by updating to the indicated resolved release. If the table does not list a corresponding resolved or unaffected release, then no ACOS release update is currently available.

ACOS Product	Releases Affected			Releases Resolved or Unaffected
ADC/CGN	4.1.4	–	4.1.4-GR1-P1	4.1.4-GR1-P2
ADC/CGN	4.1.2	–	4.1.2-Px	4.1.4-GR1-P2
ADC/CGN	4.1.1	–	4.1.1-P11	4.1.1-P12
ADC/CGN	4.1.100	–	4.1.100-P5	4.1.100-P5-SP1
ADC/CGN	4.1.0	–	4.1.0-P12	4.1.0-P13
TPS	3.2.4			3.2.4-P1
TPS	3.2.3	–	3.2.3-P4	3.2.3-P5
TPS	3.2.2	–	3.2.2-P7	3.2.2-P8
TPS	3.1.x	–	3.2.1-Px.	3.2.2-P8, 3.2.3-P5, 3.2.4-P1 [a]
ADC/CGN	2.8.2	–	2.8.2-Px	4.1.4-GR1-P2
ADC/CGN	2.7.2	–	2.7.2-Px	4.1.0-P13, 4.1.1-P12, 4.1.4-GR1-P2 [a]
ADC/CGN	2.7.1-GR1	–	2.7.1-GR1-Px	4.1.0-P13, 4.1.1-P12, 4.1.4-GR1-P2 [a]

[a] Recommended for backward, feature compatibility.

WORKAROUNDS AND MITIGATIONS

For ACOS management plane vulnerabilities, common security best practices in the industry for network appliance management and control planes can enhance protection against remote malicious attacks. Limit the exploitable attack surface for critical, infrastructure, networking equipment through the use of access lists or firewall filters to and from only trusted, administrative networks or hosts.

For potential vulnerabilities in ADC/CGN 2.x.x and TPS 3.2.1/prior management and data planes, externally blocking TCP connections with MSS values below a given threshold can be quite effective in in minimizing or negating exposures. A 500-byte MSS threshold is commonly cited in industry workarounds for CVE-2019-11478 or CVE-2019-11479.

For vulnerabilities ADC/CGN 4.1.x and TPS 3.2.2/later management planes, this method can also be applied as a mitigating technique to reduce exposures to these vulnerabilities, though it will not fully eliminate exposures for CVE-2019-11477 and CVE-2019-11478.

SOFTWARE UPDATES

Software updates that address these vulnerabilities are or will be published at the following URL:

http://www.a10networks.com/support/axseries/software-downloads

VULNERABILITY DETAILS

The following table shares brief descriptions for the vulnerabilities addressed in this document.

Vulnerability ID	Description
CVE-2019-11477	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service.
CVE-2019-11478	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences.
CVE-2019-11479	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service.
CVE-2019-5599	A vulnerability in the FreeBSD Kernel of FreeBSD could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on a targeted system. The vulnerability is due to uncontrolled resource consumption when using the Recent ACKnowledgment (RACK) TCP stack of the affected software. An attacker could exploit this vulnerability by sending a crafted sequence of Selective Acknowledgements (SACK) to the targeted system. A successful exploit could allow the attacker to cause a DoS condition on the targeted system.

RELATED LINKS

Ref #	General Link
[1]	NIST NVD, CVE-2019-11477
[2]	NIST NVD, CVE-2019-11478
[3]	NIST NVD, CVE-2019-11479
[4]	NIST NVD, CVE-2019-5599
[5]	Netflix (reporter's) Original Report - Advisory NFLX-2019-001

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2019-06-30	Initial Publication
2.0	2019-07-08	Revised 2.x.x and 3.2.1/prior L7 proxied traffic to be "likely not exposed". Corrected TPS DNS Cache Zone Updates traffic to "all' release families not exposed. Fix typos.
3.0	2019-10-11	Added 4.1.100 release chain