HTTP/2 – MULTIPLE DOS VULNERABILITIES

PUBLISHED: OCTOBER 18, 2019 | LAST UPDATE: OCTOBER 18, 2019

SUMMARY

In August 2019, multiple HTTP/2 Denial of Service (DoS) vulnerabilities were disclosed [1]. The following vulnerabilities may affect the HTTP/2 data plane of ACOS devices and are addressed in this document.

Item #	Vulnerability ID	Score Source	Score	Summary
1	CVE-2019-9512	CVSS 3.0	7.5 High	HTTP/2: flood using PING frames results in unbounded memory growth (Ping Flood) [2]
2	CVE-2019-9514	CVSS 3.0	7.5 High	HTTP/2: flood using HEADERS frames results in unbounded memory growth (Reset Flood) [3]
3	CVE-2019-9515	CVSS 3.0	7.5 High	HTTP/2: flood using SETTINGS frames results in unbounded memory growth (Settings Flood) [4]
4	CVE-2019-9518	CVSS 3.0	7.5 High	HTTP/2: flood using empty frames results in excessive resources consumption (Empty Frames Flood) [5]

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.

Releases Affected			Releases Resolved or Unaffected
5.0.0	–	5.0.0	5.0.0-P1
4.1.4	–	4.1.4-GR1-P2	4.1.4-GR1-P3

WORKAROUNDS AND MITIGATIONS

None

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-2019-9512	Some HTTP/2 implementations are vulnerable to ping floods, potentially leading to a denial of service. The attacker sends continual pings to an HTTP/2 peer, causing the peer to build an internal queue of responses. Depending on how efficiently this data is queued, this can consume excess CPU, memory, or both.
CVE-2019-9514	Some HTTP/2 implementations are vulnerable to a reset flood, potentially leading to a denial of service. The attacker opens a number of streams and sends an invalid request over each stream that should solicit a stream of RST_STREAM frames from the peer. Depending on how the peer queues the RST_STREAM frames, this can consume excess memory, CPU, or both.

CVE-2019-9515	Some HTTP/2 implementations are vulnerable to a settings flood, potentially leading to a denial of service. The attacker sends a stream of SETTINGS frames to the peer. Since the RFC requires that the peer reply with one acknowledgement per SETTINGS frame, an empty SETTINGS frame is almost equivalent in behavior to a ping. Depending on how efficiently this data is queued, this can consume excess CPU, memory, or both.
CVE-2019-9518	Some HTTP/2 implementations are vulnerable to a flood of empty frames, potentially leading to a denial of service. The attacker sends a stream of frames with an empty payload and without the end-of-stream flag. These frames can be DATA, HEADERS, CONTINUATION and/or PUSH_PROMISE. The peer spends time processing each frame disproportionate to attack bandwidth. This can consume excess CPU.

RELATED LINKS

Ref #	General Link
[1]	Netflix HTTP/2 Denial of Service Advisory
[2]	NIST NVD, CVE-2019-9512
[3]	NIST NVD, CVE-2019-9514
[3]	NIST NVD, CVE-2019-9515
[4]	NIST NVD, CVE-2019-9518

ACKNOWLEDGEMENTS

None

MODIFICATION HISTORY

Revision	Date	Description
1.0	2019-10-18	Initial Publication