HTTP/2 Vulnerability Matrix August 2019

Summary

This table lists vendors and products affected by a set of vulnerabilities in multiple HTTP/2 implementations. For more information see VU#605641, NFLX-2019-002, and vendor-specific references in the table.

For feedback on this matrix, send mail to cert@cert.org with VU#605641 in the subject.

Matrix

The list of vendors and products is not complete. It primarily contains original implementations of HTTP/2 from organizations involved in the coordinated vulnerability disclosure process.

Vendor	Product	Version Information	Data Dribble CVE-2019-9511	Ping Flood CVE-2019-9512	Resource Loop CVE-2019-9513	Reset Flood CVE-2019-9514	Settings Flood CVE-2019-9515	0-Length Headers Leak CVE-2019-9516	Internal Data Buffering CVE-2019-9517	Empty Frames Flood CVE-2019-9518
Apache	Apache HTTP Server	2.4.38 tested	Not affected	Not affected	Not affected	?	Not affected	Not affected	Affected	?
Apache	Tomcat	9.0.13 (using FreeBSD native library 1.2.16) and presumably earlier are vulnerable	Not affected	Not affected	Affected* https://markmail.org/message/konb64olyan5ye6t * just a little	Not affected	Not affected	Not affected	Not affected	Not affected
Apache	Traffic Server	?	Not affected	Affected	Not affected	Affected	Affected	Not affected	Not affected	?
Apple	macOS X	macOS X Sierra 10.12 and later are vulnerable Uses SwiftNIO	Not affected	Affected https://support.apple.com/en-gb/HT210436	Not affected	Affected https://support.apple.com/en-gb/HT210436	Affected https://support.apple.com/en-gb/HT210436	Affected https://support.apple.com/en-gb/HT210436	Not affected	Affected https://support.apple.com/en-gb/HT210436
Envoy	Envoy	Fixed in 1.11.1	Not affected	Affected https://groups.google.com/forum/#!topic/envoy-announce/ZLchtraPYVk	Affected https://groups.google.com/forum/#!topic/envoy-announce/ZLchtraPYVk	Affected https://groups.google.com/forum/#!topic/envoy-announce/ZLchtraPYVk	Affected https://groups.google.com/forum/#!topic/envoy-announce/ZLchtraPYVk	Not affected	Not affected	Affected https://groups.google.com/forum/#!topic/envoy-announce/ZLchtraPYVk
F5	nginx NGINX Plus	nginx 1.9.5 - 1.17.2 are vulnerable Fixed in 1.16.1 (stable), 1.17.3 (mainline), and NGINX Plus R18 P1	Affected http://mailman.nginx.org/pipermail/nginx-announce/2019/000249.html https://www.nginx.com/blog/nginx-updates-mitigate-august-2019-http-2-vulnerabilities/	Not affected	Affected http://mailman.nginx.org/pipermail/nginx-announce/2019/000249.html https://www.nginx.com/blog/nginx-updates-mitigate-august-2019-http-2-vulnerabilities/	Not affected	Not affected	Affected http://mailman.nginx.org/pipermail/nginx-announce/2019/000249.html https://www.nginx.com/blog/nginx-updates-mitigate-august-2019-http-2-vulnerabilities/	Not affected	Not affected
Facebook	Proxygen	?	Not affected	Affected	Affected	Affected	Affected	Not affected	Not affected	?
Google	Go net/http x/net/http2	Fixed in Go 1.12.8 and 1.11.13 Fixed in x/net/http2 v0.0.0-20190813141303-74dc4d7220e7	Not affected	Affected https://groups.google.com/forum/#!msg/golang-announce/65QixT3tcmg/DrFiG6vvCwAJ https://github.com/golang/go/issues/33606	Not affected	Affected https://groups.google.com/forum/#!msg/golang-announce/65QixT3tcmg/DrFiG6vvCwAJ https://github.com/golang/go/issues/33606	Not affected	Not affected	Not affected	Not affected
Google	gRPC C	1.21.0	Not affected	Not affected	Not affected	Affected	Affected	Not affected	Not affected	?

Google	gRPC Java	1.21.0 Uses Netty	Not affected	Not affected	Not affected	Not affected	Affected	Not affected	?	
Google	gRPC Go	1.21.0	Not affected	Not affected	Not affected	Affected	Affected	Not affected	Not affected	?
H2O Project	H2O	Fixed in 2.2.6 and 2.3.0 beta2	Not affected	Affected https://github.com/h2o/h2o/issues/2090	Not affected	Affected https://github.com/h2o/h2o/issues/2090	Affected https://github.com/h2o/h2o/issues/2090	Not affected	Not affected	Not affected
HAProxy	HAProxy	1.8 to 2.1-dev are not affected https://www.mail-archive.com/haproxy@formilux.org/msg34717.html	Not affected	Not affected	Not affected	Not affected	Not affected	Not affected	Not affected	Not affected
Hyper	Hyper: HTTP/2 for Python	https://python-hyper.org/en/latest/security.html	Not affected	Not affected	Not affected	Not affected	Not affected	Not affected	Not affected	Not affected
Istio	Istio	Fixed in 1.1.13 and 1.2.4 Uses Envoy	Not affected	Affected ISTIO-SECURITY-2019-004 https://istio.io/blog/2019/istio-security-003-004/	Affected ISTIO-SECURITY-2019-004 https://istio.io/blog/2019/istio-security-003-004/	Affected ISTIO-SECURITY-2019-004 https://istio.io/blog/2019/istio-security-003-004/	Affected ISTIO-SECURITY-2019-004 https://istio.io/blog/2019/istio-security-003-004/	Not affected	Not affected	Affected ISTIO-SECURITY-2019-004 https://istio.io/blog/2019/istio-security-003-004/
LiteSpeed	LSWS ADC OpenLiteSpeed	Fixed in: • LSWS 5.4.1 (CVE-2019-9516) • ADC 2.5.1 (CVE-2019-9516) • OpenLiteSpeed 1.5.5 and 1.4.50 (CVE-2019-9512, CVE-2019-9515, CVE-2019-9516, CVE-2019-9518)	Not affected	Affected https://blog.litespeedtech.com/2019/08/15/litespeed-addresses-http-2-dos-advisories/	Not affected	Not affected	Affected https://blog.litespeedtech.com/2019/08/15/litespeed-addresses-http-2-dos-advisories/	Affected https://blog.litespeedtech.com/2019/08/15/litespeed-addresses-http-2-dos-advisories/	Not affected	Affected https://blog.litespeedtech.com/2019/08/15/litespeed-addresses-http-2-dos-advisories/
Microsoft	Windows Internet Information Server (IIS)	Windows 10 Windows Server 2016 and 2019 Windows Server, version 1803 and version 1903	Affected https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-9511	Affected https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-9512	Affected https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-9513	Affected https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-9514	Not affected	Not affected	Not affected	Affected https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-9518
Netty Project	Netty	4.1.27 and presumably prior are vulnerable Fixed in 4.1.39	Not affected	Affected https://netty.io/news/2019/08/13/4-1-39-Final.html	Not affected	Affected https://netty.io/news/2019/08/13/4-1-39-Final.html	Affected https://netty.io/news/2019/08/13/4-1-39-Final.html	Not affected	Not affected	Affected https://netty.io/news/2019/08/13/4-1-39-Final.html
nghttp2	HTTP/2 C Library	Prior to 1.39.2 are vulnerable Fixed in 1.39.2	Affected https://github.com/nghttp2/nghttp2/releases/tag/v1.39.2	Not affected	Affected https://github.com/nghttp2/nghttp2/releases/tag/v1.39.2	Not affected	Not affected	Not affected	Not affected	Not affected
Node.js Project	Node.js	8, 10, and 12 are vulnerable	Affected https://nodejs.org/en/blog/vulnerability/aug-2019-security-releases/	Not affected	Affected https://nodejs.org/en/blog/vulnerability/aug-2019-security-releases/	Affected https://nodejs.org/en/blog/vulnerability/aug-2019-security-releases/	Not affected	?	Not affected	?

Swift	SwiftNIO HTTP/2 (swift-nio-http2)	1.0.0 - 1.4.0 are vulnerable	Not affected	Affected https://forums.swift.org/t/swiftnio-http-2-security-notice/27855	Not affected	Affected https://forums.swift.org/t/swiftnio-http-2-security-notice/27855	Affected https://forums.swift.org/t/swiftnio-http-2-security-notice/27855	Affected https://forums.swift.org/t/swiftnio-http-2-security-notice/27855	Not affected	Affected https://forums.swift.org/t/swiftnio-http-2-security-notice/27855
Twisted Matrix Labs	Twisted	16.3.0 - 19.7.0 are vulnerable	Not affected	Affected	Not affected	Affected	Affected	Not affected	Not affected	Not affected

Other References

https://blog.cloudflare.com/on-the-recent-http-2-dos-attacks/

https://blogs.akamai.com/sitr/2019/08/http2-vulnerabilities.html

https://news.ycombinator.com/item?id=20688178