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.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache</td>
<td>Apache HTTP Server</td>
<td>2.4.38 tested</td>
<td>Not affected</td>
<td>Not affected</td>
<td>Not affected</td>
<td>?</td>
<td>Not affected</td>
<td>Not affected</td>
<td>Affected</td>
<td>?</td>
</tr>
<tr>
<td>Apache</td>
<td>Tomcat</td>
<td>9.0.13 (using FreeBSD native library 1.2.16) and presumably earlier are vulnerable</td>
<td>Not affected</td>
<td>Not affected</td>
<td>Affected</td>
<td>Not affected</td>
<td>Not affected</td>
<td>Not affected</td>
<td>Not affected</td>
<td>Not affected</td>
</tr>
<tr>
<td>F5</td>
<td>nginx</td>
<td>nginx 1.9.5 - 1.17.2 are vulnerable Fixed in 1.16.1 (stable), 1.17.3 (mainline), and NGINX Plus R18 P1</td>
<td>Not affected</td>
<td>Affected</td>
<td>Not affected</td>
<td>Affected</td>
<td>Not affected</td>
<td>Not affected</td>
<td>Affected</td>
<td>Not affected</td>
</tr>
<tr>
<td>Facebook</td>
<td>Proxygen</td>
<td>?</td>
<td>Not affected</td>
<td>Affected</td>
<td>Not affected</td>
<td>Affected</td>
<td>Not affected</td>
<td>Affected</td>
<td>Not affected</td>
<td>Not affected</td>
</tr>
<tr>
<td>Software</td>
<td>Version</td>
<td>Affected Components</td>
<td>CVEs</td>
<td>Notes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
<td>---------------------</td>
<td>------</td>
<td>-------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google</td>
<td>Go gRPC C</td>
<td>1.21.0</td>
<td>Not affected</td>
<td>Not affected</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google</td>
<td>Go gRPC Java</td>
<td>1.21.0</td>
<td>Not affected</td>
<td>Not affected</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google</td>
<td>Go gRPC Go</td>
<td>1.21.0</td>
<td>Not affected</td>
<td>Not affected</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H2O Project</td>
<td>H2</td>
<td>Fixed in 2.2.6 and 2.3.0 beta2</td>
<td>Not affected</td>
<td>Affected</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HAPrxy</td>
<td>HAPrxy</td>
<td>1.8 to 2.1-dev are not affected</td>
<td>Not affected</td>
<td>Not affected</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hyper</td>
<td>Hyper: HTTP/2 for Python</td>
<td><a href="https://python-hyper.org/en/latest/security.html">https://python-hyper.org/en/latest/security.html</a></td>
<td>Not affected</td>
<td>Not affected</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Istio</td>
<td>Istio</td>
<td>Fixed in 1.1.3 and 1.2.4</td>
<td>Not affected</td>
<td>Not affected</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LiteSpeed ADC</td>
<td>OpenLiteSpeed</td>
<td>Fixed in:</td>
<td>Not affected</td>
<td>Not affected</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Windows Internet Information Server (IIS)</td>
<td>Windows 10</td>
<td>Windows 10</td>
<td>Not affected</td>
<td>Not affected</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Netty Project

Netty

4.1.27 and presumably prior are vulnerable
Fixed in 4.1.39

Not affected

Affected

Not affected


nghttp2

HTTP/2 C Library

Prior to 1.39.2 are vulnerable
Fixed in 1.39.2

Affected

Not affected

Affected

Not affected

https://github.com/nghttp2/nghttp2/releases/tag/v1.39.2

https://github.com/nghttp2/nghttp2/releases/tag/v1.39.2

https://github.com/nghttp2/nghttp2/releases/tag/v1.39.2

Node.js Project

Node.js

8, 10, and 12 are vulnerable

Affected

Not affected

Affected

Not affected


Swift

SwiftNIO HTTP/2 (swift-nio-http2)

1.0.0 - 1.4.0 are vulnerable

Not affected

Affected

Not affected

https://forums.swift.org/t/swiftnio-http-2-security-notice/27855

https://forums.swift.org/t/swiftnio-http-2-security-notice/27855

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

Not affected

https://forums.swift.org/t/swiftnio-http-2-security-notice/27855

https://forums.swift.org/t/swiftnio-http-2-security-notice/27855

https://forums.swift.org/t/swiftnio-http-2-security-notice/27855

Other References

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


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