Alpine Linux - Bug #9578

Bug # 9576 (Closed): apache2: DoS for HTTP/2 connections by continuous SETTINGS (CVE-2018-11763)

[3.8] apache2: DoS for HTTP/2 connections by continuous SETTINGS (CVE-2018-11763)

10/25/2018 09:47 AM - Alicha CH

Status:	Closed	**Start date:**	10/25/2018
Priority:	Normal	**Due date:**	
Assignee:	Kaarle Ritvanen	**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.8.2		
Affected versions:		**Security IDs:**	

Description

In Apache HTTP Server 2.4.17 to 2.4.34, by sending continuous, large SETTINGS frames a client can occupy a connection, server thread and CPU time
without any connection timeout coming to effect. This affects only HTTP/2 connections. A possible mitigation is to not enable the h2 protocol.

Fixed in Version:

Apache httpd 2.4.35

References:

https://httpd.apache.org/security/vulnerabilities_24.html

Associated revisions

Revision cd9513a2 - 10/28/2018 01:21 PM - Andy Postnikov

main/apache2: security upgrade to 2.4.35 (CVE-2018-11763)

fixes #9578

History

#1 - 10/28/2018 01:27 PM - Andy Postnikov

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:cd9513a22803b7768db28a97e5bcf9f65cceb9d2.

#2 - 10/29/2018 01:04 PM - Alicha CH

- Project changed from Alpine Security to Alpine Linux

- Category set to Security

- Status changed from Resolved to Closed

- Security IDs deleted (CVE-2018-11763)