Alpine Linux - Bug #9907

Bug # 9905 (Closed): apache2: Multiple vulnerabilities (CVE-2018-17189, CVE-2018-17199, CVE-2019-0190)

[3.8] apache2: Multiple vulnerabilities (CVE-2018-17189, CVE-2018-17199)

01/24/2019 04:44 PM - Alicha CH

Status:	Closed	**Start date:**	01/24/2019
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:**	CVE-2018-17189, CVE-2018-17199

Description

CVE-2018-17189: DoS for HTTP/2 connections via slow request bodies

By sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 connections. A possible mitigation is to not enable the h2 protocol.

Fixed In Version:

Apache httpd 2.4.38

References:

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

CVE-2018-17199: mod_session_cookie does not respect expiry time

In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session
expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

Fixed In Version:

Apache httpd 2.4.38

References:

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

Associated revisions

Revision 1d9e0b6c - 01/25/2019 07:42 PM - J0WI

main/apache2: security upgrade to 2.4.38

fixes #9907

History

#1 - 01/25/2019 07:42 PM - Anonymous

- Status changed from New to Resolved

- % Done changed from 0 to 100

Applied in changeset alpine:1d9e0b6cf8ba241e0cc1da807a574470b5aab156.

#2 - 01/28/2019 03:29 PM - Alicha CH

- Project changed from Alpine Security to Alpine Linux

- Category set to Security

- Status changed from Resolved to Closed