Alpine Linux - Bug #9547

[3.8] php5: XSS due to the header Transfer-Encoding: chunked (CVE-2018-17082)

10/09/2018 11:01 AM - Alicha CH

Status:	Closed	**Start date:**	10/09/2018
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.8.2		
Affected versions:		**Security IDs:**	

Description

The Apache2 component in PHP before 5.6.38, 7.0.x before 7.0.32, 7.1.x before 7.1.22, and 7.2.x before 7.2.10 allows XSS via the body of a "Transfer-Encoding: chunked" request,
because the bucket brigade is mishandled in the php_handler function in sapi/apache2handler/sapi_apache2.c.

Fixed In Version:

php 5.6.38, php 7.0.32, php 7.1.22, php 7.2.10

References:

https://bugs.php.net/bug.php?id=76582
https://nvd.nist.gov/vuln/detail/CVE-2018-17082

Patch:

https://github.com/php/php-src/commit/23b057742e3cf199612fa8050ae86cae675e214e

History

#1 - 10/24/2018 05:10 PM - Natanael Copa

- Status changed from New to Resolved

- % Done changed from 0 to 100

fixed with alpine:91d49cb572a9f9ed6c3d7d834a6f49d4473f3d94

#2 - 10/25/2018 07:38 AM - Alicha CH

- Project changed from Alpine Security to Alpine Linux

- Category set to Security

- Status changed from Resolved to Closed

- Security IDs deleted (CVE-2018-17082)