

Alpine Linux - Bug #9786

Bug # 9784 (Closed): phpmyadmin: Multiple vulnerabilities (CVE-2018-19968, CVE-2018-19969, CVE-2018-19970)

[3.8] phpmyadmin: Multiple vulnerabilities (CVE-2018-19968, CVE-2018-19969, CVE-2018-19970)

12/24/2018 11:43 AM - Alichia CH

Status:	Closed	Start date:	12/24/2018
Priority:	Normal	Due date:	
Assignee:		% Done:	100%
Category:	Security	Estimated time:	0.00 hour
Target version:	3.8.2	Security IDs:	CVE-2018-19968, CVE-2018-19969, CVE-2018-19970
Affected versions:			

Description

CVE-2018-19968: Local file inclusion through transformation feature.

A flaw has been found where an attacker can exploit phpMyAdmin to leak the contents of a local file. The attacker must have access to the phpMyAdmin Configuration Storage tables, although these can easily be created in any database to which the attacker has access.

An attacker must have valid credentials to log in to phpMyAdmin; this vulnerability does not allow an attacker to circumvent the login system.

Affected Versions:

phpMyAdmin versions from at least 4.0 through 4.8.3 are affected

Reference:

<https://www.phpmyadmin.net/security/PMASA-2018-6/>

Patch:

<https://github.com/phpmyadmin/phpmyadmin/commit/6a1ba61e29002f0305a9322a8af4eaaeb11c0732>

CVE-2018-19969: XSRF/CSRF vulnerability

By deceiving a user to click on a crafted URL, it is possible to perform harmful SQL operations such as renaming databases, creating new tables/routines, deleting designer pages, adding/deleting users, updating user passwords, killing SQL processes, etc.

Affected Versions

phpMyAdmin versions 4.7.0 through 4.7.6 and 4.8.0 through 4.8.3 are affected.

Reference:

<https://www.phpmyadmin.net/security/PMASA-2018-7/>

Patches:

see <https://www.phpmyadmin.net/security/PMASA-2018-7/>

CVE-2018-19970: XSS vulnerability in navigation tree

A Cross-Site Scripting vulnerability was found in the navigation tree, where an attacker can deliver a payload to a user through a specially-crafted database/table name.

Affected Versions

phpMyAdmin versions from at least 4.0 through 4.8.3 are affected

Reference:

<https://www.phpmyadmin.net/security/PMASA-2018-8/>

Patch:

<https://github.com/phpmyadmin/phpmyadmin/commit/b293ff5f234ef493336ed8638f623a12164d359e>

Associated revisions

Revision 70ea79c1 - 01/08/2019 10:46 AM - Leonardo Arena

community/phpmyadmin: security upgrade to 4.8.4

CVE-2018-19968, CVE-2018-19969, CVE-2018-19970

Fixes #9786

History

#1 - 01/08/2019 10:47 AM - Anonymous

- *Status changed from New to Resolved*

- *% Done changed from 0 to 100*

Applied in changeset [alpine:70ea79c1c7c3e2187967fb04101d410b1d749390](#).

#2 - 01/09/2019 07:17 AM - Alichia CH

- *Project changed from Alpine Security to Alpine Linux*

- *Category set to Security*

- *Status changed from Resolved to Closed*