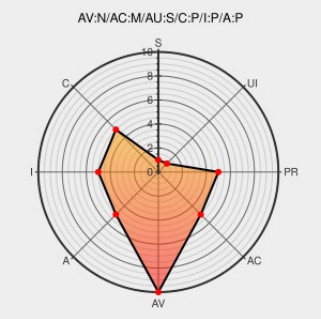
CVE-2013-3238

Published on: 04/25/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:30 PM UTC

CVE-2013-3238

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Phpmyadmin from Phpmyadmin contain the following vulnerability:

phpMyAdmin 3.5.x before 3.5.8 and 4.x before 4.0.0-rc3 allows remote authenticated users to execute arbitrary code via a /e\x00 sequence, which is not properly handled before making a preg_replace function call within the "Replace table prefix" feature.

CVE-2013-3238 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 6 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Prevent null-byte injection in preg_replace() · phpmyadmin/phpmyadmin@ffa720d · GitHub	github.com text/html	CONFIRM github.com/phpmyadmin/phpmyadmin/commit/ffa720d90a79c1f33cf4c5a3
Support / Security / Advisories / / MDVSA-2013:160 | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2013:160
phpMyAdmin - Security - PMASA-2013-2	www.phpmyadmin.net text/html	CONFIRM www.phpmyadmin.net/home_page/security/PMASA-2013-2
NEOHAPSIS - Peace of Mind Through Integrity and Insight	web.archive.org text/html Inactive Link Not Archived	BUGTRAQ 20130424 [waraxe-2013-SA#103] - Multiple Vulnerabilities
Support/Advisories/MGASA-2013-0133 - Mageia wiki	wiki.mageia.org text/html	CONFIRM wiki.mageia.org/en/Support/Advisories/MGASA-2013-0133

[SECURITY] Fedora 17 Update: phpMyAdmin-3.5.8.1-1.fc17	lists.fedoraproject.org text/html	FEDORA FEDORA-2013-7000
Dropped unsafe usage of preg_replace · phpmyadmin/phpmyadmin@dedd542 · GitHub	github.com text/html	CONFIRM github.com/phpmyadmin/phpmyadmin/commit/dedd542cdaf1606ca9aa3f
phpMyAdmin Authenticated Remote Code Execution via preg_replace()	www.exploit-db.com Proof of Concept text/x-ruby	EXPLOIT-DB 25136
openSUSE-SU-2013:1065-1: moderate: update for phpMyAdmin	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:1065
[SECURITY] Fedora 19 Update: phpMyAdmin-3.5.8.1-1.fc19	lists.fedoraproject.org text/html	FEDORA FEDORA-2013-6928
[SECURITY] Fedora 18 Update: phpMyAdmin-3.5.8.1-1.fc18	lists.fedoraproject.org text/html	FEDORA FEDORA-2013-6977

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Phpmyadmin	Phpmyadmin	3.5.0.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.5.1.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.5.2.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.5.2.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.5.2.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.5.3.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.5.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.5.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.5.6	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.5.7	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.5.7	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	3.5.8	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.0	rc2	All	All
Application	Phpmyadmin	Phpmyadmin	3.5.0.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.5.1.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.5.2.0	All	All	All

Application	Phpmyadmin	Phpmyadmin	3.5.2.1	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.5.2.2	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.5.3.0	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.5.4	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.5.5	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.5.6	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.5.7	All	All	All
Application	Phpmyadmin	Phpmyadmin	3.5.7	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	3.5.8	rc1	All	All
Application	Phpmyadmin	Phpmyadmin	4.0.0	rc2	All	All

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.4:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.5:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.6:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.7:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.7:rc1:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.8:rc1:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.0:rc2:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.4:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.5:*:*:*:*:*:*:*

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.6:*:*:*:*:*:*:*

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.7:*:*:*:*:*:*:*

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.7:rc1:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.5.8:rc1:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:4.0.0:rc2:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→