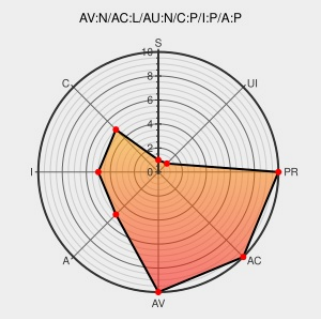
# CVE-2009-1149

Published on: 03/26/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:27 PM UTC

## CVE-2009-1149

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




Certain versions of Phpmyadmin from Phpmyadmin contain the following vulnerability:

CRLF injection vulnerability in bs_disp_as_mime_type.php in the BLOB streaming feature in phpMyAdmin before 3.1.3.1 allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via the (1) c_type and possibly (2) file_type parameters.

CVE-2009-1149 has been assigned by cve@mitre.org to track the vulnerability

### CVSS2 Score: 7.5 - HIGH

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| PARTIAL | PARTIAL | PARTIAL |

### CVE References

| Description | Tags | Link |
|---|---|---|
| 404 Not Found | Patch, phpmyadmin.svn.sourceforge.net, text/html, Inactive Link, Not Archived | MISC phpmyadmin.svn.sourceforge.net/viewvc/phpmyadmin/branches/MAINT_3_1_3/phpMyAdmin r1=12303&r2=12302&pathrev=12303 |
| SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Information - Secunia.com | web.archive.org, text/html | SECUNIA 34642 |

| | | |
|---|---|---|
| phpMyAdmin File Inclusion and HTTP Response Splitting - Secunia Advisories - Vulnerability Information - Secunia.com | web.archive.org<br>text/html | SECUNIA 34468 |
| phpMyAdmin - Security - PMASA-2009-1 | Patch<br>Vendor Advisory<br>www.phpmyadmin.net<br>text/html | CONFIRM www.phpmyadmin.net/home_page/security/PMASA-2009-1.php |
| [security-announce] SUSE Security Summary Report: SUSE-SR:2009:008 | lists.opensuse.org<br>text/html | SUSE SUSE-SR:2009:008 |



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 | 3.1.0 | All | All | All |
| Application | Phpmyadmin | Phpmyadmin | 3.1.0.0 | All | All | All |
| Application | Phpmyadmin | Phpmyadmin | 3.1.1 | All | All | All |
| Application | Phpmyadmin | Phpmyadmin | 3.1.1 | rc1 | All | All |
| Application | Phpmyadmin | Phpmyadmin | 3.1.2 | All | All | All |
| Application | Phpmyadmin | Phpmyadmin | 3.1.2 | rc1 | All | All |
| Application | Phpmyadmin | Phpmyadmin | 3.1.3 | rc1 | All | All |
| Application | Phpmyadmin | Phpmyadmin | 3.1.0 | All | All | All |
| Application | Phpmyadmin | Phpmyadmin | 3.1.0.0 | All | All | All |
| Application | Phpmyadmin | Phpmyadmin | 3.1.1 | All | All | All |
| Application | Phpmyadmin | Phpmyadmin | 3.1.1 | rc1 | All | All |
| Application | Phpmyadmin | Phpmyadmin | 3.1.2 | All | All | All |
| Application | Phpmyadmin | Phpmyadmin | 3.1.2 | rc1 | All | All |
| Application | Phpmyadmin | Phpmyadmin | 3.1.3 | rc1 | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Phpmyadmin | Phpmyadmin | All | All | All | All |

cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.1:rc1:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.2:rc1:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.3:rc1:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.1:rc1:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.2:rc1:*:*:*:*:*:*:

cpe:2.3:a:phpmyadmin:phpmyadmin:3.1.3:rc1:*:*:*:*:*:*:

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→