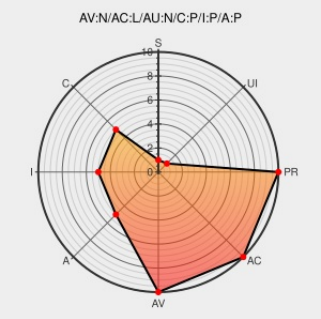
CVE-2013-1803

Published on: 05/05/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:33 PM UTC

CVE-2013-1803

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



Certain versions of Php-fusion from Php-fusion contain the following vulnerability:

Multiple SQL injection vulnerabilities in PHP-Fusion before 7.02.06 allow remote attackers to execute arbitrary SQL commands via the (1) orderby parameter to downloads.php; or remote authenticated users with certain permissions to execute arbitrary SQL commands via a (2) parameter name starting with "delete_attach_" in an edit action to forum/postedit.php; the (3) poll_opts[] parameter in a newthread action to forum/postnewthread.php; the (4) pm_email_notify, (5) pm_save_sent, (6) pm_inbox, (7) pm_sentbox, or (8) pm_savebox parameter to administration/settings_messages.php; the (9) thumb_compression, (10) photo_watermark_text_color1, (11) photo_watermark_text_color2, or (12) photo_watermark_text_color3 parameter to administration/settings_photo.php; the (13) enable parameter to administration/bbcodes.php; the (14) news_image, (15) news_image_t1, or (16) news_image_t2 parameter to administration/news.php; the (17) news_id parameter in an edit action to administration/news.php; or the (18) article_id parameter in an edit action to administration/articles.php. NOTE: the user ID cookie issue in Authenticate.class.php is already covered by CVE-2013-7375.

CVE-2013-1803 has been assigned by secalert@redhat.com 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

No Description Provided	osvdb.org Inactive Link Not Archived	OSVDB 90693
News: PHPFusion v7.02.06 - Official Home of the PHPFusion CMS	Vendor Advisory www.php-fusion.co.uk text/html	CONFIRM www.php-fusion.co.uk/news.php?readmore=569
No Description Provided	osvdb.org Inactive Link Not Archived	OSVDB 90709
PHP-Fusion 7.02.05 XSS / LFI / SQL Injection ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/120598/PHP-Fusion-7.02.05-XSS-LFI-SQL-Injection.html
oss-security - Re: CVE request: PHP-Fusion waraxe-2013-SA#097	www.openwall.com text/html	MLIST [oss-security] 20130302 Re: CVE request: PHP-Fusion waraxe-2013-SA#097
No Description Provided	osvdb.org Inactive Link Not Archived	OSVDB 90713
[waraxe-2013-SA#097] - Multiple Vulnerabilities in PHP-Fusion 7.02.05	www.waraxe.us text/html	MISC www.waraxe.us/advisory-97.html
oss-security - CVE request: PHP-Fusion waraxe-2013-SA#097	www.openwall.com text/html	MLIST [oss-security] 20130303 CVE request: PHP-Fusion waraxe-2013-SA#097
No Description Provided	osvdb.org Inactive Link Not Archived	OSVDB 90711
No Description Provided	osvdb.org Inactive Link Not Archived	OSVDB 90712
No Description Provided	osvdb.org Inactive Link Not Archived	OSVDB 90695
No Description Provided	osvdb.org Inactive Link Not Archived	OSVDB 90714
Security Advisory SA52403 - PHP-Fusion Multiple SQL Injection and Cross-Site Scripting Vulnerabilities - Secunia	Vendor Advisory web.archive.org text/html	SECUNIA 52403
Full Disclosure: [waraxe-2013-SA#097] - Multiple Vulnerabilities in PHP-Fusion 7.02.05	seclists.org text/html	FULLDISC 20130228 [waraxe-2013-SA#097] - Multiple Vulnerabilities in PHP-Fusion 7.02.05
No Description Provided	osvdb.org Inactive Link Not Archived	OSVDB 90710

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Php-fusion	Php-fusion	7.02.01	All	All	All
Application	Php-fusion	Php-fusion	7.02.02	All	All	All
Application	Php-fusion	Php-fusion	7.02.03	All	All	All
Application	Php-fusion	Php-fusion	7.02.04	All	All	All
Application	Php-fusion	Php-fusion	7.02.01	All	All	All
Application	Php-fusion	Php-fusion	7.02.02	All	All	All
Application	Php-fusion	Php-fusion	7.02.03	All	All	All
Application	Php-fusion	Php-fusion	7.02.04	All	All	All
Application	Php-fusion	Php-fusion	All	All	All	All

cpe:2.3:a:php-fusion:php-fusion:7.02.01:*:*:*:*:*:*:*:

cpe:2.3:a:php-fusion:php-fusion:7.02.02:*:*:*:*:*:*:*:

cpe:2.3:a:php-fusion:php-fusion:7.02.03:*:*:*:*:*:*:*:

cpe:2.3:a:php-fusion:php-fusion:7.02.04:*:*:*:*:*:*:*:

cpe:2.3:a:php-fusion:php-fusion:7.02.01:*:*:*:*:*:*:*:

cpe:2.3:a:php-fusion:php-fusion:7.02.02:*:*:*:*:*:*:*:

cpe:2.3:a:php-fusion:php-fusion:7.02.03:*:*:*:*:*:*:*:

cpe:2.3:a:php-fusion:php-fusion:7.02.04:*:*:*:*:*:*:*:

cpe:2.3:a:php-fusion:php-fusion:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→