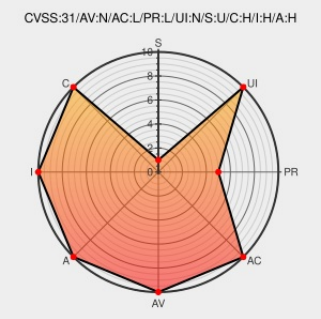
CVE-2020-12461

Published on: 04/29/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:35 PM UTC

CVE-2020-12461

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



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

PHP-Fusion 9.03.50 allows SQL Injection because maincore.php has an insufficient protection mechanism. An attacker can develop a crafted payload that can be inserted into the sort_order GET parameter on the members.php members search page. This parameter allows for control over anything after the ORDER BY clause in the SQL query.

CVE-2020-12461 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.5 - MEDIUM

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

CVE References

Description	Tags	Link
#2308 - Solution (Small fixes) · php-fusion/PHP-Fusion@858e43d · GitHub	Patch Third Party Advisory web.archive.org	MISC github.com/php-fusion/PHP-Fusion/commit/858e43d7b0ea1897f76d5bcb3a1aed438132c0e2

	text/html Inactive Link Not Archived	
#2308 - Solution (clean up) · php-fusion/PHP-Fusion@d95cd4a · GitHub	Patch Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC github.com/php-fusion/PHP-Fusion/commit/d95cd4a2d22487723266c898b98e6be10754e03d
Shitter Writeup (Difficulty 3/3) - HackMD	Exploit Third Party Advisory hackmd.io text/html	MISC hackmd.io/lq7nA3ISSoeiGjiHVn5CoA
#2308 - Solution (clean up) · php-fusion/PHP-Fusion@79fe5ec · GitHub	Patch Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC github.com/php-fusion/PHP-Fusion/commit/79fe5ec1d5c75e017a6f42127741b9543658f822
Authenticated SQL Injection Exists in any page that allows control over the sort order. · Issue #2308 · php-fusion/PHP-Fusion · GitHub	Exploit Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC github.com/php-fusion/PHP-Fusion/issues/2308

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	9.03.50	All	All	All
Application	Php-fusion	Php-fusion	9.03.50	All	All	All

cpe:2.3:a:php-fusion:php-fusion:9.03.50:*:*:*:*:*:*:*:

cpe:2.3:a:php-fusion:php-fusion:9.03.50:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report