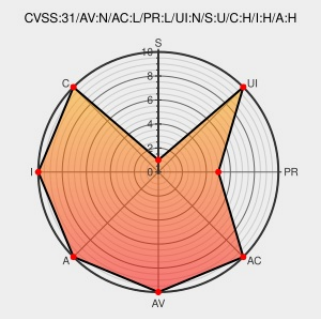
CVE-2018-15139

Published on: 08/13/2018 12:00:00 AM UTC

Last Modified on: 02/10/2022 07:23:00 AM UTC

CVE-2018-15139

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



Certain versions of Openemr from Open-emr contain the following vulnerability:

Unrestricted file upload in interface/super/manage_site_files.php in versions of OpenEMR before 5.0.1.4 allows a remote authenticated attacker to execute arbitrary PHP code by uploading a file with a PHP extension via the images upload form and accessing it in the images directory.

CVE-2018-15139 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
OpenEMR patches serious vulnerabilities uncovered by Project Insecurity	Third Party Advisory www.databreaches.net text/html	MISC www.databreaches.net/openemr-patches-serious-vulnerabilities-uncovered-by-p insecurity/

Insecurity		
OpenEMR 5.0.1.3 Shell Upload ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/163110/OpenEMR-5.0.1.3-Shell-Upload.html
Exploits/CVE-2018-15139-Exploit at main · Hacker5preme/Exploits · GitHub	github.com text/html	MISC github.com/Hacker5preme/Exploits/tree/main/CVE-2018-15139-Exploit
OpenEMR 5.0.1.3 Shell Upload ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/163482/OpenEMR-5.0.1.3-Shell-Upload.html
security fixes by bradymiller · Pull Request #1757 · openemr/openemr · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/openemr/openemr/pull/1757/commits/c2808a0493243f618bbbb3459af23c7da

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Open-emr	Openemr	All	All	All	All
Application	Open-emr	Openemr	All	All	All	All

cpe:2.3:a:open-emr:openemr:*:*:*:*:*:*:*:*:

cpe:2.3:a:open-emr:openemr:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→