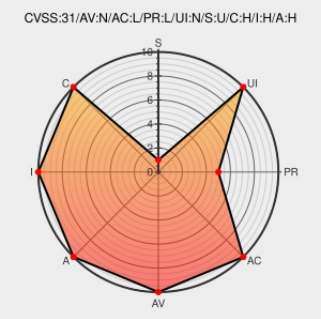
CVE-2019-14530

Published on: 08/13/2019 12:00:00 AM UTC

Last Modified on: 02/10/2022 03:26:00 PM UTC

CVE-2019-14530

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



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

An issue was discovered in custom/ajax_download.php in OpenEMR before 5.0.2 via the fileName parameter. An attacker can download any file (that is readable by the user www-data) from server storage. If the requested file is writable for the www-data user and the directory /var/www/openemr/sites/default/documents/cqm_qrda/ exists, it will be deleted from server.

CVE-2019-14530 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 - MEDIUM

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

CVE References

Description	Tags	Link
OpenEMR 5.0.1.7 Path Traversal ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/163215/OpenEMR-

		5.0.1.7-Path-Traversal.html
Exploits/CVE-2019-14530-Exploit at main · Hacker5preme/Exploits · GitHub	github.com text/html	MISC github.com/Hacker5preme/Exploits/tree/main/CVE-2019-14530-Exploit
GitHub - Wezery/CVE-2019-14530: OpenEMR security issue	Third Party Advisory github.com text/html	MISC github.com/Wezery/CVE-2019-14530
OpenEMR 5.0.1.7 Path Traversal ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/163375/OpenEMR-5.0.1.7-Path-Traversal.html
bug fixins by bradymiller · Pull Request #2592 · openemr/openemr · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/openemr/openemr/pull/2592

There are currently no QIDs associated with this CVE

Exploit/POC from Github

OpenEMR < 5.0.2 - (Authenticated) Path Traversal - Local File Disclosure

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

Social Mentions

Source	Title	Posted (UTC)
@pwnwikiorg	CVE-2019-14530 OpenEMR 5.0.1.7 - 'fileName' 目錄遍歷漏洞 pwnwiki.org/index.php?titl…	2021-06-21 13:55:30
@SEC_IT_Cyber	OpenEMR CVE-2019-14530 exploit ?? OpenEMR < 5.0.2 - (Authenticated) Path Traversal - Local File Disclosure ?? OpenE… twitter.com/i/web/status/1…	2021-07-03 09:11:00

← Previous ID

Next ID→

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