



CVE-2018-15140

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

Last Modified on: 03/23/2021 11:24:27 PM UTC

CVE-2018-15140

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Openemr](#) from [Open-emr](#) contain the following vulnerability:

Directory traversal in portal/import_template.php in versions of OpenEMR before 5.0.1.4 allows a remote attacker authenticated in the patient portal to read arbitrary files via the "docid" parameter when the mode is set to get.

CVE-2018-15140 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

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-project-insecurity/
OpenEMR 5.0.1.3 - (Authenticated) Arbitrary File	Exploit	EXPLOIT-DB 45202

Actions - Linux webapps Exploit

Third Party Advisory

VDB Entry

www.exploit-db.com

Proof of Concept

text/html

fix path by bradymiller · Pull Request #1765 · openemr/openemr · GitHub

Patch

Third Party Advisory

github.com

text/html

 CONFIRM github.com/openemr/openemr/pull/1765/files

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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 →