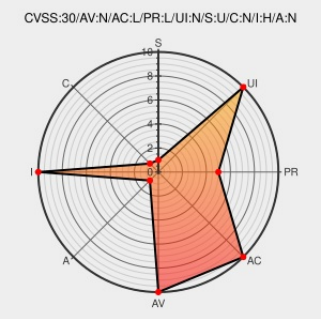
CVE-2018-10572

Published on: 04/30/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:22 PM UTC

CVE-2018-10572

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



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

interface/patient_file/letter.php in OpenEMR before 5.0.1 allows remote authenticated users to bypass intended access restrictions via the newtemplatename and form_body parameters.

CVE-2018-10572 has been assigned by 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	NONE	HIGH	NONE

CVSS2 Score: 5.5 - MEDIUM

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

CVE References

Description	Tags	Link
security fixes (#1519) · openemr/openemr@699e3c2 · GitHub	Patch, Third Party Advisory, github.com, text/html	MISC github.com/openemr/openemr/commit/699e3c2ef68545357cac714505df1419b8

Security issues reported by outside group · Issue #1518 · openemr/openemr · GitHub	Issue Tracking Third Party Advisory github.com text/html	MISC github.com/openemr/openemr/issues/1518
Release Features - OpenEMR Project Wiki	Vendor Advisory www.open-emr.org text/html	MISC www.open-emr.org/wiki/index.php/Release_Features#Version_5.0.1
security fixes by bradymiller · Pull Request #1519 · openemr/openemr · GitHub	Issue Tracking Third Party Advisory github.com text/html	MISC github.com/openemr/openemr/pull/1519
OpenEMR 弱點分析 – 資安最前線	Exploit Third Party Advisory csticsfrontline.wordpress.com text/html	MISC csticsfrontline.wordpress.com/2018/05/24/openemr-%E5%BC%B1%E9%BB%9E%E5%88%86%E6%9E%90/

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→