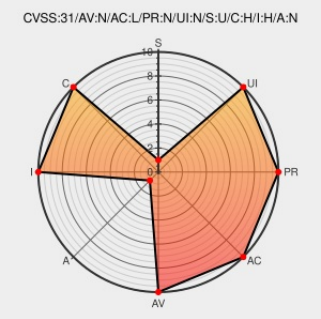
CVE-2018-15152

Published on: 08/15/2018 12:00:00 AM UTC

Last Modified on: 02/10/2022 07:24:00 AM UTC

CVE-2018-15152

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



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

Authentication bypass vulnerability in portal/account/register.php in versions of OpenEMR before 5.0.1.4 allows a remote attacker to access (1) portal/add_edit_event_user.php, (2) portal/find_appt_popup_user.php, (3) portal/get_allergies.php, (4) portal/get_amendments.php, (5) portal/get_lab_results.php, (6) portal/get_medications.php, (7) portal/get_patient_documents.php, (8) portal/get_problems.php, (9) portal/get_profile.php, (10) portal/portal_payment.php, (11) portal/messaging/messages.php, (12) portal/messaging/secure_chat.php, (13) portal/report/pat_ledger.php, (14) portal/report/portal_custom_report.php, or (15) portal/report/portal_patient_report.php without authenticating as a patient.

CVE-2018-15152 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.1 - CRITICAL

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

CVSS2 Score: 6.4 - MEDIUM

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

CVE References

Description	Tags	Link
OpenEMR Patches - OpenEMR Project Wiki	Patch Vendor Advisory www.open-emr.org text/html	CONFIRM www.open-emr.org/wiki/index.php/OpenEMR_Patches
Exploits/CVE-2018-15152-Exploit at main · Hacker5preme/Exploits · GitHub	github.com text/html	MISC github.com/Hacker5preme/Exploits/tree/main/CVE-2018-15152-Exploit
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/
6 Best VPN Services in Canada Reviewed (2021) - Speed & Security Tests	Technical Description Third Party Advisory insecurity.sh application/pdf	MISC insecurity.sh/reports/openemr.pdf
OpenEMR 5.0.1.3 Authentication Bypass ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/163181/OpenEMR-5.0.1.3-Authentication-Bypass.html
PP2 Update by sjpadgett · Pull Request #1758 · openemr/openemr · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/openemr/openemr/pull/1758/files

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→

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