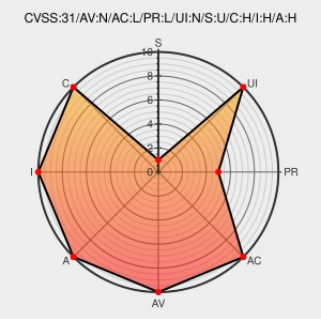
CVE-2020-36243

Published on: 02/07/2021 12:00:00 AM UTC

Last Modified on: 06/01/2021 05:44:00 PM UTC

CVE-2020-36243

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



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

The Patient Portal of OpenEMR 5.0.2.1 is affected by a Command Injection vulnerability in /interface/main/backup.php. To exploit the vulnerability, an authenticated attacker can send a POST request that executes arbitrary OS commands via shell metacharacters.

CVE-2020-36243 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: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
OpenEMR Patches - OpenEMR Project Wiki	Patch Vendor Advisory www.open-emr.org text/html	MISC www.open-emr.org/wiki/index.php/OpenEMR_Patches

OpenEMR 5.0.2 Patch 5 has been released - News - OpenEMR Community	community.open-emr.org text/html	MISC community.open-emr.org/t/openemr-5-0-2-patch-5-has-been-released/15431
SonarSource Blog	Exploit Third Party Advisory blog.sonarsource.com text/html	MISC blog.sonarsource.com/openemr-5-0-2-1-command-injection-vulnerability
OpenEMR 5.0.2.1: Command Injection vulnerability puts health records at risk - Tech Stories - SonarSource Community	community.sonarsource.com text/html	MISC community.sonarsource.com/t/openemr-5-0-2-1-command-injection-vulnerability-puts-health-records-at-risk/33592

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	5.0.2.1	All	All	All
Application	Open-emr	Openemr	5.0.2.1	All	All	All

cpe:2.3:a:open-emr:openemr:5.0.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:open-emr:openemr:5.0.2.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@LinInfoSec	Php - CVE-2020-36243: blog.sonarsource.com/openemr-5-0-2-…	2021-05-28 15:10:33

← Previous ID

Next ID→