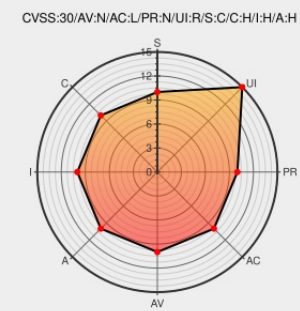
CVE-2020-13563

Published on: 02/01/2021 12:00:00 AM UTC

Last Modified on: 07/29/2022 02:24:00 PM UTC

CVE-2020-13563

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



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

A cross-site scripting vulnerability exists in the template functionality of phpGACL 3.3.7. A specially crafted HTTP request can lead to arbitrary JavaScript execution. An attacker can provide a crafted URL to trigger this vulnerability in the phpGACL template group_id parameter.

CVE-2020-13563 has been assigned by talos-cna@cisco.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.1 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
TALOS-2020-1177 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	Exploit, Technical Description, Third Party Advisory, talosintelligence.com, text/html	MISC talosintelligence.com/vulnerability_reports/TALOS-2020-1177

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	5.0.2	All	All	All
Application	Open-emr	Openemr	5.0.2	All	All	All
Application	Phpgacl Project	Phpgacl	3.3.7	All	All	All
Application	Phpgacl Project	Phpgacl	3.3.7	All	All	All

cpe:2.3:a:open-emr:openemr:5.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:open-emr:openemr:5.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:phpgacl_project:phpgacl:3.3.7:*:*:*:*:*:*:*:

cpe:2.3:a:phpgacl_project:phpgacl:3.3.7:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@RemotelyAlerts	Severity: ?? | A cross-site scripting vulnerability exi... | CVE-2020-13563 | Link for more: alerts.remotelyrmm.com/CVE-2020-13563	2022-07-29 15:33:30

← Previous ID

Next ID→