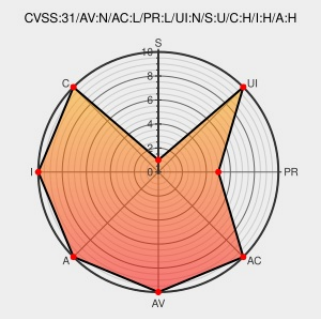
CVE-2023-27486

Published on: Not Yet Published

Last Modified on: 03/15/2023 02:12:00 PM UTC

CVE-2023-27486 - advisory for GHSA-hpxg-7428-6jvv

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



Certain versions of Xcat from Xcat Project contain the following vulnerability:

xCAT is a toolkit for deployment and administration of computer clusters. In versions prior to 2.16.5 if zones are configured as a mechanism to secure clusters in XCAT, it is possible for a local root user from one node to obtain credentials to SSH to any node in any zone, except the management node of the default zone. XCAT zones are not enabled by default. Only users that use the optional zone feature are impacted. All versions of xCAT prior to xCAT 2.16.5 are vulnerable. This problem has been fixed in xCAT 2.16.5. Users making use of zones should upgrade to 2.16.5. Users unable to upgrade may mitigate the issue by disabling zones or patching the management node with the fix contained in commit `85149c37f49`.

CVE-2023-27486 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **xcat2** - **xcat-core** version **= < 2.16.5**

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

CVE References

Description	Tags	Link
Unsufficient check in credentials.pm · Issue #7246 · xcat2/xcat-core · GitHub	github.com text/html	MISC github.com/xcat2/xcat-core/issues/7246
Have server enforce SSH zone separation by jjohnson42 · Pull Request #7247 · xcat2/xcat-core ·	github.com text/html	MISC github.com/xcat2/xcat-core/pull/7247

GitHub		
Insufficient authorization validation between zones when xCAT zones are enabled · Advisory · xcat2/xcat-core · GitHub	github.com text/html	MISC github.com/xcat2/xcat-core/security/advisories/GHSA-hpxg-7428-6jvv
Have server enforce SSH zone separation by jjohnson42 · Pull Request #7247 · xcat2/xcat-core · GitHub	github.com text/html	MISC github.com/xcat2/xcat-core/pull/7247/commits/85149c37f49dbca7bd85f1f586960315604fc024

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	Xcat Project	Xcat	All	All	All	All

cpe:2.3:a:xcat_project:xcat:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-27486 : xCAT is a toolkit for deployment and administration of computer clusters. In versions prior to 2.1… twitter.com/i/web/status/1…	2023-03-08 19:06:01
/r/netcve	CVE-2023-27486	2023-03-08 20:38:55

← Previous ID

Next ID→