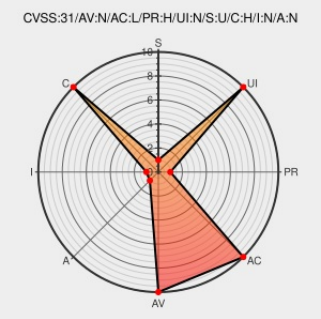
CVE-2021-3417

Published on: 03/09/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:53 PM UTC

CVE-2021-3417 - advisory for LEN-49884

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



Certain versions of Xclarity Orchestrator from Lenovo contain the following vulnerability:

An internal product security audit of LXCO, prior to version 1.2.2, discovered that credentials for Lenovo XClarity Administrator (LXCA), if added as a Resource Manager, are encoded then written to an internal LXCO log file each time a session is established with LXCA. Affected logs are captured in the First Failure Data Capture (FFDC) service log. The FFDC service log is only generated when requested by a privileged LXCO user and it is only accessible to the privileged LXCO user that requested the file.

CVE-2021-3417 has been assigned by psirt@lenovo.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Lenovo** - **XClarity Orchestrator** version **< 1.2.2**

CVSS3 Score: 4.9 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
Lenovo XClarity Orchestrator (LXCO) Information Disclosure Vulnerabilities - Lenovo Support US	Vendor Advisory support.lenovo.com text/html	MISC support.lenovo.com/us/en/product_security/LEN-49884

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lenovo	Xclarity Orchestrator	All	All	All	All
Application	Lenovo	Xclarity Orchestrator	All	All	All	All

cpe:2.3:a:lenovo:xclarity_orchestrator:*:*:*:*:*:*:*:*:

cpe:2.3:a:lenovo:xclarity_orchestrator:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→