CVE-2017-3743

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-3743
State	PUBLISHED
Assigner	lenovo
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-20 00:29:00 UTC
Updated	2025-04-20 01:37:25 UTC
Description	If multiple users are concurrently logged into a single system where one user is sending a command via the Lenovo ToolsC

Risk And Classification

Primary CVSS: v3.0 7.5 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

Problem Types: CWE-200 | Sensitive information disclosure

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	3.5		AV:N/AC:M/Au:S/C:P/I:N/A:N

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

Single

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:M/Au:S/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lenovo	Advanced Settings Utility	All	All	All	All
Application	Lenovo	Toolscenter Dynamic System Analysis	All	All	All	All
Application	Lenovo	Updatexpress System Pack Installer	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Lenovo Group Ltd.	ToolsCenter	affected Lenovo Advanced Settings Utility versions earlier than 10.2 and UXSPI and DSA versic

References

Reference	Source
Credentials sent through the Lenovo ToolsCenter may be exposed to local users - Lenovo Support US	af854a3a-2127-422b-91ae-364da26
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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