CVE-2017-3801

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

Summary

CVE	CVE-2017-3801
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-02-15 20:59:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	A vulnerability in the web-based GUI of Cisco UCS Director 6.0.0.0 and 6.0.0.1 could allow an authenticated, local attacker

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Unified Computing System Director	6.0.0.0	All	All	All
Application	Cisco	Unified Computing System Director	6.0.0.1	All	All	All
Application	Cisco	Unified Computing System Director	6.0.0.0	All	All	All
Application	Cisco	Unified Computing System Director	6.0.0.1	All	All	All

References

Reference
Cisco UCS Director Privilege Escalation Vulnerability
Cisco Unified Computing System Director Developer Menu RBAC Flaw Lets Remote Authenticated Users Gain Elevated Privileges - SecurityT
Cisco UCS Director CVE-2017-3801 Local Privilege Escalation Vulnerability
CVE Program record
NVD vulnerability detail

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