



CVE-2018-0148

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2018-0148
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-02-22 00:29:00 UTC
Updated	2019-10-09 23:31:00 UTC
Description	A vulnerability in the web-based management interface of Cisco UCS Director Software and Cisco Integrated Management

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Ucs Director	6.5(0.0.65832)	All	All	All
Application	Cisco	Ucs Director	6.5\0.0.65832\	All	All	All
Application	Cisco	Ucs Director	6.5\0.0.65832\	All	All	All

References

Reference	Source
Malformed Request	BID
Cisco UCS Director and Cisco Integrated Management Controller Supervisor Cross-Site Request Forgery Vulnerability	CONFIRM
Cisco UCS Director Access Control Flaw Lets Remote Users Conduct Cross-Site Request Forgery Attacks - SecurityTracker	SECTrack
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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)