



CVE-2020-3240

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

Summary

CVE	CVE-2020-3240
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-15 21:15:00 UTC
Updated	2020-04-21 19:45:00 UTC
Description	Multiple vulnerabilities in the REST API of Cisco UCS Director and Cisco UCS Director Express for Big Data may allow a re

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Ucs Director	6.0.0.0	All	All	All
Application	Cisco	Ucs Director	6.0.0.1	All	All	All
Application	Cisco	Ucs Director	6.0.1.0	All	All	All
Application	Cisco	Ucs Director	6.0.1.1	All	All	All
Application	Cisco	Ucs Director	6.0.1.2	All	All	All
Application	Cisco	Ucs Director	6.0.1.3	All	All	All
Application	Cisco	Ucs Director	6.5.0.0	All	All	All
Application	Cisco	Ucs Director	6.5.0.1	All	All	All
Application	Cisco	Ucs Director	6.5.0.2	All	All	All
Application	Cisco	Ucs Director	6.5.0.3	All	All	All
Application	Cisco	Ucs Director	6.5.0.4	All	All	All
Application	Cisco	Ucs Director	6.6.0.0	All	All	All
Application	Cisco	Ucs Director	6.6.1.0	All	All	All
Application	Cisco	Ucs Director	6.6.2.0	All	All	All
Application	Cisco	Ucs Director	6.7.0.0	All	All	All
Application	Cisco	Ucs Director	6.7.1.0	All	All	All
Application	Cisco	Ucs Director	6.7.2.0	All	All	All

Application	Cisco	Ucs Director	6.7.3.0	All	All	All
Application	Cisco	Ucs Director	6.0.0.0	All	All	All
Application	Cisco	Ucs Director	6.0.0.1	All	All	All
Application	Cisco	Ucs Director	6.0.1.0	All	All	All
Application	Cisco	Ucs Director	6.0.1.1	All	All	All
Application	Cisco	Ucs Director	6.0.1.2	All	All	All
Application	Cisco	Ucs Director	6.0.1.3	All	All	All
Application	Cisco	Ucs Director	6.5.0.0	All	All	All
Application	Cisco	Ucs Director	6.5.0.1	All	All	All
Application	Cisco	Ucs Director	6.5.0.2	All	All	All
Application	Cisco	Ucs Director	6.5.0.3	All	All	All
Application	Cisco	Ucs Director	6.5.0.4	All	All	All
Application	Cisco	Ucs Director	6.6.0.0	All	All	All
Application	Cisco	Ucs Director	6.6.1.0	All	All	All
Application	Cisco	Ucs Director	6.6.2.0	All	All	All
Application	Cisco	Ucs Director	6.7.0.0	All	All	All
Application	Cisco	Ucs Director	6.7.1.0	All	All	All
Application	Cisco	Ucs Director	6.7.2.0	All	All	All
Application	Cisco	Ucs Director	6.7.3.0	All	All	All
Application	Cisco	Ucs Director Express For Big Data	All	All	All	All

References

Reference	Source	Link	Tags
ZDI-20-542 Zero Day Initiative	MISC	www.zerodayinitiative.com	Third
Multiple Vulnerabilities in Cisco UCS Director and Cisco UCS Director Express for Big Data	CISCO	tools.cisco.com	Vend
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

No vendor comments have been submitted for this CVE.

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

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](#).

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