



CVE-2019-15253

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

Summary

CVE	CVE-2019-15253
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-05 18:15:00 UTC
Updated	2021-12-21 12:53:00 UTC
Description	A vulnerability in the web-based management interface of Cisco Digital Network Architecture (DNA) Center could allow an attacker to execute arbitrary code on the affected device. The vulnerability is caused by a cross-site scripting (XSS) flaw in the user interface. An attacker could exploit this vulnerability by sending a specially crafted request to the affected device. The attacker would need to be authenticated to the device and have access to the user interface. The vulnerability affects all versions of the software prior to 1.3.1.4. Cisco has released a patch for this vulnerability in version 1.3.1.4 of the software.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Dna Center	All	All	All	All
Application	Cisco	Dna Center	All	All	All	All

References

Reference	Source	Link	Tags
Cisco Digital Network Architecture Center 1.3.1.4 Cross Site Scripting ~ Packet Storm	MISC	packetstormsecurity.com	
Cisco Digital Network Architecture Center Stored Cross-Site Scripting Vulnerability	CISCO	tools.cisco.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, authoritative

No vendor comments have been submitted for this CVE.

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

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