

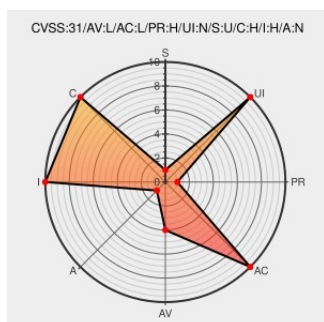


CVE-2021-1558

Published on: 05/22/2021 12:00:00 AM UTC

Last Modified on: 05/27/2021 08:10:00 PM UTC

CVE-2021-1558 - advisory for cisco-sa-dnasp-conn-prvesc-q6T6BzW

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Dna Spaces](#) from [Cisco](#) contain the following vulnerability:

Multiple vulnerabilities in Cisco DNA Spaces Connector could allow an authenticated, local attacker to elevate privileges and execute arbitrary commands on the underlying operating system as root. These vulnerabilities are due to insufficient restrictions during the execution of affected CLI commands. An attacker could exploit these vulnerabilities

by leveraging the insufficient restrictions during execution of these commands. A successful exploit could allow the attacker to elevate privileges from dnasadmin and execute arbitrary commands on the underlying operating system as root.

CVE-2021-1558 has been assigned by [Cisco](#) psirt@cisco.com to track the vulnerability - currently rated as **MEDIUM** severity.

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of these vulnerabilities that are described in this advisory.

Affected Vendor/Software: [Cisco](#) **Cisco - Cisco DNA Spaces Connector** version n/a

CVSS3 Score: **6.7 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	HIGH	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.2 - HIGH**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact

COMPLETE

COMPLETE

COMPLETE

CVE References

Description	Tags	Link
Cisco DNA Spaces Connector Privilege Escalation Vulnerabilities	tools.cisco.com text/html	CISCO 20210519 Cisco DNA Spaces Connector Privilege Escalation Vulnerabilities

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Dna Spaces	_connector	All	All	All
cpe:2.3:a:cisco:dna_spaces\:_connector:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
X @CVEreport	CVE-2021-1558 : Multiple vulnerabilities in Cisco DNA Spaces Connector could allow an authenticated, local attack... twitter.com/i/web/status/1...	2021-05-22 06:55:01
reddit /r/netcve	CVE-2021-1558	2021-05-22 07:41:59

[← Previous ID](#)[Next ID →](#)

© [CVE.report](#) 2023 [X](#) [N](#) |

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](#).

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