

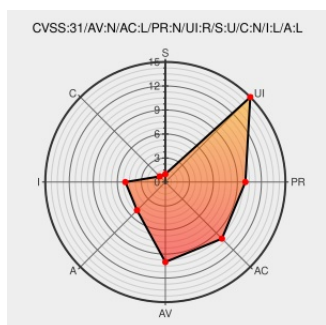


CVE-2020-3597

Published on: 10/08/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:39 PM UTC

CVE-2020-3597 - advisory for cisco-sa-ndb-path-traversal-wVDyXZPy

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

Certain versions of [Nexus Data Broker](#) from [Cisco](#) contain the following vulnerability:

A vulnerability in the configuration restore feature of Cisco Nexus Data Broker software could allow an unauthenticated, remote attacker to perform a directory traversal attack on an affected device. The vulnerability is due to insufficient validation of configuration backup files. An attacker could exploit this vulnerability by persuading an

administrator to restore a crafted configuration backup file. A successful exploit could allow the attacker to overwrite arbitrary files that are accessible through the affected software on an affected device.

CVE-2020-3597 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 the vulnerability that is described in this advisory.

Affected Vendor/Software: [Cisco](#) **Cisco - Cisco Nexus Data Broker** version n/a

CVSS3 Score: **5.4 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	LOW	LOW

CVSS2 Score: **5.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact

NONE

PARTIAL

PARTIAL

CVE References

Description

Tags

Link

Cisco Nexus Data Broker Software Path Traversal Vulnerability

Vendor Advisory
tools.cisco.com
text/html

 [CISCO 20201007 Cisco Nexus Data Broker Software Path Traversal Vulnerability](#)

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	Nexus Data Broker	All	All	All	All
Application	Cisco	Nexus Data Broker	All	All	All	All
cpe:2.3:a:cisco:nexus_data_broker:*****:						
cpe:2.3:a:cisco:nexus_data_broker:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#)