

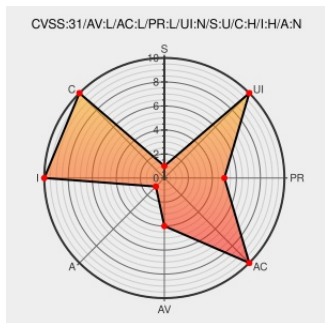


CVE-2020-3483

Published on: 10/14/2020 12:00:00 AM UTC

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

CVE-2020-3483 - advisory for DUO-PSA-2020-004

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

Certain versions of [Duo Network Gateway](#) from [Cisco](#) contain the following vulnerability:

Duo has identified and fixed an issue with the Duo Network Gateway (DNG) product in which some customer-provided SSL certificates and private keys were not excluded from logging. This issue resulted in certificate and private key information being written out in plain-text to local files on the DNG host. Any private keys logged in this way could

be viewed by those with access to the DNG host operating system without any need for reversing encrypted values or similar techniques. An attacker that gained access to the DNG logs and with the ability to intercept and manipulate network traffic between a user and the DNG, could decrypt and manipulate SSL/TLS connections to the DNG and to the protected applications behind it. Duo Network Gateway (DNG) versions 1.3.3 through 1.5.7 are affected.

CVE-2020-3483 has been assigned by [Cisco](#) psirt@cisco.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Cisco](#) **Cisco - Duo Network Gateway (DNG)** version < 1.5.8

CVSS3 Score: **6.3 - MEDIUM**

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

CVSS2 Score: **3.3 - LOW**

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

PARTIAL

PARTIAL

NONE

CVE References

Description	Tags	Link
DUO-PSA-2020-004: Duo Product Security Advisory Duo Security	Patch Vendor Advisory duo.com text/html	 CISCO Duo Network Gateway (DNG) Information Disclosure 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	Duo Network Gateway	All	All	All	All

cpe:2.3:a:cisco:duo_network_gateway:*:*:*:*:*:*

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](#)