



CVE-2020-3556

Published on: 11/06/2020 12:00:00 AM UTC

Last Modified on: 11/07/2023 03:22:00 AM UTC

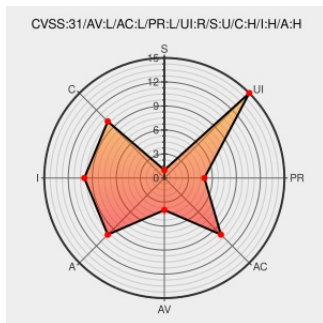
CVE-2020-3556 - advisory for cisco-sa-anyconnect-ipc-KfQO9QhK

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Anyconnect Secure Mobility Client](#) from [Cisco](#) contain the following vulnerability:

A vulnerability in the interprocess communication (IPC) channel of Cisco AnyConnect Secure Mobility Client Software could allow an authenticated, local attacker to cause a targeted AnyConnect user to execute a malicious script. The vulnerability is due to a lack of authentication to the IPC listener. An attacker could exploit this

vulnerability by sending crafted IPC messages to the AnyConnect client IPC listener. A successful exploit could allow an attacker to cause the targeted AnyConnect user to execute a script. This script would execute with the privileges of the targeted AnyConnect user. In order to successfully exploit this vulnerability, there must be an ongoing AnyConnect session by the targeted user at the time of the attack. To exploit this vulnerability, the attacker would also need valid user credentials on the system upon which the AnyConnect client is being run. Cisco has not released software updates that address this vulnerability.

CVE-2020-3556 has been assigned by [Cisco](#) psirt@cisco.com to track the vulnerability - currently rated as **HIGH** severity.

The Cisco Product Security Incident Response Team (PSIRT) is aware that proof-of-concept exploit code is available for the vulnerability described in this advisory.

Affected Vendor/Software: [Cisco](#) **Cisco - Cisco AnyConnect Secure Mobility Client** version n/a

CVSS3 Score: **7.3 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **4.4 - MEDIUM**

Access Vector	Access Complexity	Authentication
---------------	-------------------	----------------

vector	complexity	
LOCAL	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Cisco AnyConnect Secure Mobility Client Arbitrary Code Execution Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20201104 Cisco AnyConnect Secure Mobility Client Arbitrary Code Execution 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	Anyconnect Secure Mobility Client	4.9\3052\	All	All	All
Application	Cisco	Anyconnect Secure Mobility Client	98.145\86\	All	All	All
Application	Cisco	Anyconnect Secure Mobility Client	4.9\3052\	All	All	All
Application	Cisco	Anyconnect Secure Mobility Client	98.145\86\	All	All	All
cpe:2.3:a:cisco:anyconnect_secure_mobility_client:4.9\3052\:*:*:*:*:*:						
cpe:2.3:a:cisco:anyconnect_secure_mobility_client:98.145\86\:*:*:*:*:*:						
cpe:2.3:a:cisco:anyconnect_secure_mobility_client:4.9\3052\:*:*:*:*:*:						
cpe:2.3:a:cisco:anyconnect_secure_mobility_client:98.145\86\:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @yipcw	Cisco fixes 6-month-old AnyConnect VPN zero-day with exploit code CVE-2020-3556 bleepingcomputer.com/news/security/...	2021-05-13 17:24:00
 @tempest_sec	A Cisco publicou correções para a vulnerabilidade CVE-2020-3556 (CVSS 7.3) que trata de uma falha no canal de comun... twitter.com/i/web/status/1...	2021-05-14 15:06:10
 @mschlenker	@Cisco_Germany @Cisco CVE-2020-3556?	2021-07-07 19:26:18
	Anyconnect zero day exploit effect on openconnect	2021-05-31

[← 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](#)