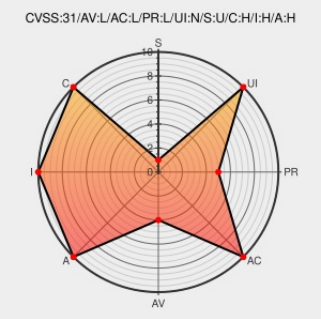
CVE-2020-3433

Published on: 08/17/2020 12:00:00 AM UTC

Last Modified on: 01/31/2023 05:25:00 PM UTC

CVE-2020-3433 - advisory for cisco-sa-anyconnect-dll-F26WwJW

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 for Windows could allow an authenticated, local attacker to perform a DLL hijacking attack. To exploit this vulnerability, the attacker would need to have valid credentials on the Windows system. The vulnerability is due to insufficient validation of resources that are loaded by the application at run time. An attacker could exploit this vulnerability by sending a crafted IPC message to the AnyConnect process. A successful exploit could allow the attacker to execute arbitrary code on the affected machine with SYSTEM privileges. To exploit this vulnerability, the attacker would need to have valid credentials on the Windows system.

CVE-2020-3433 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as HIGH 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 AnyConnect Secure Mobility Client** version **n/a**

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	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 AnyConnect Secure Mobility Client for Windows DLL Hijacking Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20200805 Cisco AnyConnect Secure Mobility Client for Windows DLL Hijacking Vulnerability
Cisco AnyConnect Privilege Escalation ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/159420/Cisco-AnyConnect-Privilege-Escalation.html

There are currently no QIDs associated with this CVE

Exploit/POC from Github

PoCs and technical analysis of three vulnerabilities found on Cisco AnyConnect for Windows: CVE-2020-3433, CVE-2020-3…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Anyconnect Secure Mobility Client	All	All	All	All
Application	Cisco	Anyconnect Secure Mobility Client	All	All	All	All

cpe:2.3:a:cisco:anyconnect_secure_mobility_client:*:*:*:*:*:windows:*:*:

cpe:2.3:a:cisco:anyconnect_secure_mobility_client:*:*:*:*:*:windows:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CyberWarship	PoCs for CVE-2020-3433, CVE-2020-3434, and CVE-2020-3435 'PoCs and technical details for the three vulnerabilities… twitter.com/i/web/status/1…	2021-08-14 09:37:04
@ipssignatures	The vuln CVE-2020-3433 has a tweet created 0 days ago and retweeted 14 times. twitter.com/CyberWarship/s… #pow1rtrtwwcve	2021-08-14 13:06:00
@hebilisim	Fundamentals matter. Introducing crypto's first economic calendar for traders. CVE-2020-3433	2022-07-05 11:04:58
@inthewildio	CVE-2020-3433 is getting exploited #inthewild. Find out more at inthewild.io/vuln/CVE-2020-… CVE-2020-3153 is getting ex… twitter.com/i/web/status/1…	2022-10-25 06:02:32

@avoidthehack	CISA Adds Six Known Exploited Vulnerabilities to Catalog CVE-2020-3433, CVE-2020-3153 (Cisco Anyconnect) CVE-2018… twitter.com/i/web/status/1…	2022-10-25 16:30:01
@ohhara_shiojiri	"The Cisco product vulnerabilities are CVE-2020-3433 and CVE-2020-3153,"	2022-10-26 04:12:21
@buherator	CVE-2020-3433 and CVE-2020-3153 are apparently still alive and well (neat bugs too!) twitter.com/BleepinCompute…	2022-10-26 06:11:24
@SecurityWeek	Cisco Confirms In-the-Wild Exploitation of Two VPN Vulnerabilities - CVE-2020-3433 and CVE-2020-3153https://www.sec… twitter.com/i/web/status/1…	2022-10-26 10:41:02
@MrsYisWhy	SecurityWeek: Cisco Confirms In-the-Wild Exploitation of Two VPN Vulnerabilities - CVE-2020-3433 and CVE-2020-3153https://ift.tt/YalkDFV	2022-10-26 10:44:55
@CycuraMX	Las dos fallas de seguridad (registradas como CVE-2020-3433 y CVE-2020-3153) permiten a los atacantes: Realizar… twitter.com/i/web/status/1…	2022-10-26 14:01:53
@EchelonEyes	Хакеры активно используют уязвимости Cisco AnyConnect двухлетней давности Недостатки CVE-2020-3153 и CVE-2020-3433… twitter.com/i/web/status/1…	2022-10-26 14:07:06
@cert_ist	Deux vulnérabilités impactant #Cisco #AnyConnect découvertes en 2020 (CVE-2020-3433 et CVE-2020-3153) sont exploité… twitter.com/i/web/status/1…	2022-10-26 14:59:37
@ipssignatures	The vuln CVE-2020-3433 has a tweet created 0 days ago and retweeted 12 times. twitter.com/SecurityWeek/s… #pow1rtrtwwcve	2022-10-26 18:06:01
@SecurityWeek	Cisco Confirms In-the-Wild Exploitation of Two VPN Vulnerabilities - CVE-2020-3433 and CVE-2020-3153https://www.sec… twitter.com/i/web/status/1…	2022-10-27 02:01:00
@MrsYisWhy	SecurityWeek: Cisco Confirms In-the-Wild Exploitation of Two VPN Vulnerabilities - CVE-2020-3433 and CVE-2020-3153https://ift.tt/YalkDFV	2022-10-27 02:04:32
@ipssignatures	The vuln CVE-2020-3433 has a tweet created 0 days ago and retweeted 10 times. twitter.com/SecurityWeek/s… #pow1rtrtwwcve	2022-10-27 06:06:00
@KanzumoITCo	AnyConnect VPNs Under Active Cyberattack: (CVE-2020-3433, with a CVSS score of 7.8) could allow a logged-in user to… twitter.com/i/web/status/1…	2022-10-27 11:44:28
@CVEtrends	Top 3 trending CVEs on Twitter Past 24 hrs: CVE-2022-34718: 320.9K (audience size) CVE-2020-3433: 264.8K CVE-2020-… twitter.com/i/web/status/1…	2022-10-27 13:00:02
@motakasoft	GitHub Trending Archive, 28 Oct 2022, C#. goichot/CVE-2020-3433, Green-Software-Foundation/carbon-aware-sdk, kodlam… twitter.com/i/web/status/1…	2022-10-30 10:30:06
@seconize_co	CISA ALERT! CVE-2020-3433 (Uncontrolled Search Path) - #KnowYourSCORE now --> riskscore.info/cve/CVE-2020-3…… twitter.com/i/web/status/1…	2022-10-31 04:35:00
@motakasoft	GitHub Trending Archive, 29 Oct 2022, C#. goichot/CVE-2020-3433, DeadlyKitten/MonkeModManager, n00mkrad/text2image-… twitter.com/i/web/status/1…	2022-10-31 10:30:05
@Paradoxinfosec	2/3 The vulnerabilities, identified as CVE-2020-3153 (CVSS score: 6.5) and CVE-2020-3433 (CVSS score: 7.8), could a… twitter.com/i/web/status/1…	2022-10-31 17:21:40
@omarbv	Cisco AnyConnect Secure Mobility Client for Windows DLL Hijacking Vulnerability ? CVE-2020-3433 ? 7.8 CVSS v3 tools.cisco.com/security/cente…	2022-10-31 22:21:55
@iototsecnews	Cisco AnyConnect の脆弱性 CVE-2020-3433 などの悪用を検出：CISA KEV リストにも追加 #security #cisco #vulnerability #cisa iototsecnews.jp/2022/10/25/cis…	2022-10-31 23:12:21
@Syynya	Cisco AnyConnect の脆弱性 CVE-2020-3433 などの悪用を検出：CISA KEV リストにも追加 iototsecnews.jp/2022/10/25/cis… @iototsecnewsより	2022-11-01 01:15:11

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report