



# 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 [Cisco](#) 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 | <div>Vendor Advisory</div> <div>tools.cisco.com</div> <div>text/html</div> |  CISCO 20200805 Cisco AnyConnect Secure Mobility Client for Windows DLL Hijacking Vulnerability |
| Cisco AnyConnect Privilege Escalation ≈ Packet Storm                            | <div>packetstormsecurity.com</div> <div>text/html</div>                    |  MISC packetstormsecurity.com/files/159420/Cisco-AnyConnect-Privilege-Escalation.html           |

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](mailto:comment@cve.report).

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... <a href="#">twitter.com/i/web/status/1...</a>                         | 2021-08-14 09:37:04 |
|  @ipssignatures | The vuln CVE-2020-3433 has a tweet created 0 days ago and retweeted 14 times. <a href="#">twitter.com/CyberWarship/s...</a> #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 <a href="#">inthewild.io/vuln/CVE-2020-...</a> CVE-2020-3153 is getting ex... <a href="#">twitter.com/i/web/status/1...</a> | 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... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>                                                  | 2022-10-25<br>16:30:01 |
|  @ohhara_shiojiri  | "The Cisco product vulnerabilities are CVE-2020-3433 and CVE-2020-3153,"                                                                                                                                                                                | 2022-10-26<br>04:12:21 |
|  @buherator        | CVE-2020-3433 and CVE-2020-3153 are apparently still alive and well (neat bugs too!) <a href="https://twitter.com/BleepinCompute...">twitter.com/BleepinCompute...</a>                                                                                  | 2022-10-26<br>06:11:24 |
|  @SecurityWeek     | Cisco Confirms In-the-Wild Exploitation of Two VPN Vulnerabilities - CVE-2020-3433 and CVE-2020-3153 <a href="https://www.sec...">https://www.sec...</a> <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>              | 2022-10-26<br>10:41:02 |
|  @MrsYisWhy        | SecurityWeek: Cisco Confirms In-the-Wild Exploitation of Two VPN Vulnerabilities - CVE-2020-3433 and CVE-2020-3153 <a href="https://ift.tt/YalkDFV">https://ift.tt/YalkDFV</a>                                                                          | 2022-10-26<br>10:44:55 |
|  @CycuraMX         | Las dos fallas de seguridad (registradas como CVE-2020-3433 y CVE-2020-3153) permiten a los atacantes: Realizar... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>                                                    | 2022-10-26<br>14:01:53 |
|  @EchelonEyes      | Хакеры активно используют уязвимости Cisco AnyConnect двухлетней давности Недостатки CVE-2020-3153 и CVE-2020-3433... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>                                                 | 2022-10-26<br>14:07:06 |
|  @cert_ist         | Deux vulnérabilités impactant #Cisco #AnyConnect découvertes en 2020 (CVE-2020-3433 et CVE-2020-3153) sont exploité... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>                                                | 2022-10-26<br>14:59:37 |
|  @ipssignatures    | The vuln CVE-2020-3433 has a tweet created 0 days ago and retweeted 12 times. <a href="https://twitter.com/SecurityWeek/s...">twitter.com/SecurityWeek/s...</a> #pow1rtrtwcve                                                                           | 2022-10-26<br>18:06:01 |
|  @SecurityWeek     | Cisco Confirms In-the-Wild Exploitation of Two VPN Vulnerabilities - CVE-2020-3433 and CVE-2020-3153 <a href="https://www.sec...">https://www.sec...</a> <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>              | 2022-10-27<br>02:01:00 |
|  @MrsYisWhy      | SecurityWeek: Cisco Confirms In-the-Wild Exploitation of Two VPN Vulnerabilities - CVE-2020-3433 and CVE-2020-3153 <a href="https://ift.tt/YalkDFV">https://ift.tt/YalkDFV</a>                                                                          | 2022-10-27<br>02:04:32 |
|  @ipssignatures  | The vuln CVE-2020-3433 has a tweet created 0 days ago and retweeted 10 times. <a href="https://twitter.com/SecurityWeek/s...">twitter.com/SecurityWeek/s...</a> #pow1rtrtwcve                                                                           | 2022-10-27<br>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... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>                                                | 2022-10-27<br>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-... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>                                                 | 2022-10-27<br>13:00:02 |
|  @motakasoft     | GitHub Trending Archive, 28 Oct 2022, C#. goichot/CVE-2020-3433, Green-Software-Foundation/carbon-aware-sdk, kodlam... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>                                                | 2022-10-30<br>10:30:06 |
|  @seconize_co    | CISA ALERT! CVE-2020-3433 (Uncontrolled Search Path) - #KnowYourSCORE now --> <a href="https://riskscore.info/cve/CVE-2020-3...">riskscore.info/cve/CVE-2020-3...</a> <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> | 2022-10-31<br>04:35:00 |
|  @motakasoft     | GitHub Trending Archive, 29 Oct 2022, C#. goichot/CVE-2020-3433, DeadlyKitten/MonkeModManager, n00mkrad/text2image-... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>                                                | 2022-10-31<br>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... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>                                                | 2022-10-31<br>17:21:40 |
|  @omarbv         | Cisco AnyConnect Secure Mobility Client for Windows DLL Hijacking Vulnerability ? CVE-2020-3433 ? 7.8 CVSS v3 <a href="https://tools.cisco.com/security/cente...">tools.cisco.com/security/cente...</a>                                                 | 2022-10-31<br>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 <a href="https://iototsecnews.jp/2022/10/25/cis...">iototsecnews.jp/2022/10/25/cis...</a>                                                         | 2022-10-31<br>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 <a href="https://iototsecnews.jp/2022/10/25/cis...">iototsecnews.jp/2022/10/25/cis...</a> @iototsecnewsより                                                                               | 2022-11-01<br>01:15:11 |

© [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](#)