Security Advisory 2020-058

Cisco AnyConnect Secure Mobility Client Vulnerability

December 8, 2020 — v1.0

TLP:WHITE

Summary

Cisco released an advisory on the 4th of December regarding a vulnerability in the interprocess communication (IPC) channel of Cisco AnyConnect Secure Mobility Client Software. It could allow an authenticated local attacker to cause a targeted AnyConnect user to execute a malicious script.

Technical Details

The vulnerability was assigned *CVE-2020-3556* with a CVSS score of 7.3 [1].

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.

Products Affected

This vulnerability affects all versions of the Cisco AnyConnect Secure Mobility Client Software for the following platforms if they have a vulnerable configuration:

- AnyConnect Secure Mobility Client for Windows
- AnyConnect Secure Mobility Client for MacOS
- AnyConnect Secure Mobility Client for Linux

This vulnerability does not affect Cisco AnyConnect Secure Mobility Client for the Apple iOS and Android platforms.

Recommendations

Cisco will release free software updates that will address the vulnerability described in this advisory.

CERT-EU recommends updating Cisco AnyConnect Secure Mobility Clients once an update is available.

Workarounds

The recommended workaround is to upgrade to *Release 4.9.04053* and edit the `AnyConnectLocalPolicy.xml` file to set `RestrictScriptWebDeploy` to **true**. Ensure that `BypassDownloader` is set to **false**. The new `AnyConnectLocalPolicy.xml` file would then be deployed to end machines using an out-of-band method of deployment.

There are additional configuration settings for Release 4.9.04053 and later that are strongly recommended to be set for increased protection [2].

References

[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-ipc-KfQO9QhK/

[2] https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect49/release/notes/release-notes-anyconnect-4-9.html#Cisco_Reference.dita_79c2fd57-db64-4449-9072-26e62e46630b