CVE-2020-3432:

Cisco AnyConnect Secure Mobility Client file corruption

Vairav Advisory Report

Date: 2025-02-12

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: mail@vairavtech.com

EXECUTIVE SUMMARY

A vulnerability, identified as CVE-2020-3432, has been discovered in Cisco AnyConnect Secure Mobility Client for macOS. This vulnerability allows an authenticated, local attacker to cause a denial-of-service (DoS) condition by deleting arbitrary files on the system. Exploitation could lead to service disruption and potential data loss.

VULNERABILITY DETAILS

CVE-2020-3432

- **Description:** This vulnerability is due to improper validation of directory paths in the affected application. An authenticated, local attacker could exploit this vulnerability by creating a symbolic link (symlink) from a critical system file to a directory within the application's file path. When the application attempts to delete its own directory, it would follow the symlink and delete the targeted system file, leading to a denial-of-service condition.
- **Impact:** Successful exploitation allows the attacker to delete arbitrary files on the system, potentially causing system instability, application crashes, and loss of critical data, resulting in a denial-of-service condition.
- **CVSS Score:** 5.6 (Medium)

AFFECTED VERSIONS

Cisco AnyConnect Secure Mobility Client for macOS versions earlier than 4.9.00086 are affected by this vulnerability.

EXPLOIT DETAILS

To exploit this vulnerability, an attacker must have valid local user credentials and the ability to create symlinks on the macOS system. By creating a symlink from a critical system file to a directory used by the AnyConnect application, the attacker can cause the application to delete the system file during its normal operations, leading to a denial-of-service condition.

RECOMMENDED ACTIONS

Patch & Upgrade:

Cisco has released software updates to address this vulnerability. Users are advised to upgrade to Cisco AnyConnect Secure Mobility Client for macOS version 4.9.00086 or later.

ADDITIONAL SECURITY MEASURES

- **Restrict user privileges** – Limit user permissions to prevent unauthorized modification of system files.
- **Use application whitelisting** – Prevent unauthorized executables from running, including modified uninstallers.
- **Monitor system logs** – Use tools like Wazuh or native macOS logging to detect unusual file modifications.

REFERENCES

- https://app.opencve.io/cve/CVE-2020-3432
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-mac-dos-36s2y3Lv

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: mail@vairavtech.com

Website: https://vairavtech.com