CVE-2025-20206: Cisco Secure Client for Windows with Secure Firewall Posture Engine DLL Hijacking Vulnerability

Vairav CVE Report

Date: 2025-03-06

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Thirbam Sadak 148
Baluwatar, Kathmandu

EXECUTIVE SUMMARY

A vulnerability, identified as **CVE-2025-20206**, has been discovered in Cisco Secure Client for Windows with the Secure Firewall Posture Engine installed. This vulnerability allows an authenticated local attacker to perform a DLL hijacking attack, potentially leading to arbitrary code execution with SYSTEM privileges. The vulnerability has been assigned a **CVSS score of 7.1**, categorizing it as High severity. Exploitation of this vulnerability could result in full system compromise.

VULNERABILITY DETAILS

CVE-2025-20206

- **Description:** The vulnerability exists due to insufficient validation of resources loaded by the application at runtime. An authenticated local attacker with valid user credentials can exploit this vulnerability by sending a crafted inter-process communication (IPC) message to a specific Cisco Secure Client process, leading to DLL hijacking and execution of arbitrary code with SYSTEM privileges.
- **Impact:** Successful exploitation allows attackers to execute arbitrary code on the affected machine with SYSTEM privileges, potentially leading to full system compromise.
- **CVSS Score:** 7.1 (High)

AFFECTED VERSIONS

Cisco Secure Client for Windows versions earlier than 5.1.8.105 with the Secure Firewall Posture Engine installed are affected by this vulnerability.

EXPLOIT DETAILS

To exploit this vulnerability, an attacker must have valid user credentials on the Windows system and the ability to send crafted IPC messages to the Cisco Secure Client process. Successful exploitation could lead to arbitrary code execution with SYSTEM privileges, resulting in full system compromise.

RECOMMENDED ACTIONS

Patch & Upgrade:

Upgrade to Cisco Secure Client for Windows version 5.1.8.105 or later to address this vulnerability.

ADDITIONAL SECURITY MEASURES

- **Restrict Access**: Limit user access to systems running Cisco Secure Client to trusted individuals only.
- **Monitor Systems**: Regularly monitor systems for unusual activity that may indicate exploitation attempts.

REFERENCES

- https://app.opencve.io/cve/CVE-2025-20206
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-secure-dll-injection-AOyzEqSg

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: sales@vairavtech.com

Website: https://vairavtech.com