مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

High-Severity Vulnerability in Cisco Secure Client

Tracking #:432316937

Date:06-03-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in the interprocess communication (IPC) channel of Cisco Secure Client for Windows. This vulnerability could allow a local, authenticated attacker to perform a DLL hijacking attack, leading to arbitrary code execution with SYSTEM privileges.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-20206**
- CVSS Score: Base 7.1 High
- A security vulnerability exists in the interprocess communication (IPC) channel of Cisco Secure Client for Windows. This vulnerability allows an authenticated, local attacker to perform a DLL hijacking attack on an affected device when the Secure Firewall Posture Engine (formerly HostScan) is installed.
- This vulnerability arises due to insufficient validation of resources that are loaded by the application at run time. A local attacker with valid user credentials could exploit this issue by sending a crafted IPC message to a specific Cisco Secure Client process.
- Successful exploitation may result in arbitrary code execution with SYSTEM privileges, posing a significant risk to affected devices.

Affected Products:

- Cisco Secure Client for Windows with the Secure Firewall Posture Engine installed.
- Versions earlier than 5.1.8.105 are vulnerable.

Fixed Versions:

- Cisco Secure Client version 5.1.8.105 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Cisco.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-secure-dll-injection-AOyzEqSg