Cisco Secure Client for Windows - DLL Hijacking Vulnerability

Overview

A DLL hijacking vulnerability (CVE-2025-20206) was found in Cisco Secure Client for Windows which could allow an authenticated, local attacker to execute arbitrary code with SYSTEM privileges. This issue stems from insufficient validation of resources loaded at runtime. Exploitation requires valid user credentials and a crafted IPC message to a specific process.

CVE-2025-20206 (CVSS 7.1) allows an attacker with local access and valid credentials to execute arbitrary code on an affected system by leveraging a DLL hijacking flaw in the **Secure Firewall Posture Engine**. The attack does not require user interaction and has a low complexity, making it easier to exploit.

Affected Products

- Vulnerable - Cisco Secure Client for Windows with Secure Firewall Posture Engine.
- Not Affected - Secure Client for Linux, macOS, iOS, Android, and Universal Windows Platform.

If successful, the attacker can gain full control over the compromised machine. The impact would be devastating - affecting both confidentiality and integrity by allowing for unauthorized code execution and system manipulation.

Aspire Protects

- **Patch** - Cisco has released updates that fix this vulnerability. Please see Cisco's advisory for patch guidance.
- Limit user permissions to prevent unauthorized access.

TTPs to Watch

Execution

- Hijack Execution Flow [T1574] – The attacker may use DLL hijacking to run malicious code.

Privilege Escalation

- Abuse Elevation Control Mechanism [T1548.002] – The attacker may escalate privileges to SYSTEM.

IoCs

There are no known IoCs associated with the above vulnerability at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

This vulnerability could impact any industry that relies on Cisco Secure Client for Windows with the Secure Firewall Posture Engine for endpoint security and network access control. The vulnerability may impact the following industries/sectors:

- Finance
- Healthcare
- Government
- Manufacturing
- Retail
- Energy
- Education
- Telecommunications
- And others

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**

- The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
- Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Cisco Secure Client for Windows with Secure Firewall Posture Engine DLL Hijacking Vulnerability