Cisco IP Phone Vulnerability Could Expose Sensitive Information in Enterprise Environments

Overview

A vulnerability, tracked as CVE-2025-20158, CVSS 4.4) in the debug shell of Cisco Video Phone 8875 and Cisco Desk Phone 9800 Series could allow an authenticated, local attacker to access sensitive information on an affected device. Successful exploitation requires the attacker to have valid administrative credentials with SSH access, which is disabled by default.

This issue is due to insufficient validation of user-supplied input in the debug shell. An attacker could exploit this by sending a crafted SSH client command to the CLI, leading to unauthorized access to sensitive information within the device's operating system.

Affected Products

- Cisco Video Phone 8875
- Cisco Desk Phone 9800 Series
- Devices running vulnerable versions of Cisco SIP IP Phone Software with SSH access enabled.

Cisco has released software updates to address this vulnerability. No workarounds are available, therefore, Aspire recommends patching as soon as possible.

Aspire Protects

- **Patch –** Cisco has released Cisco SIP Software 3.3(1) as the first fixed version.
- Disable SSH access if not required, as it is disabled by default.
- Monitor administrative access logs for any unauthorized SSH activity.

TTPs to Watch

Credential Access

- Brute Force [T1110] – The attacker may attempt to brute-force administrative credentials to gain access.

Execution

- Command and Scripting Interpreter [T1059] – The attacker may exploit the debug shell to execute unauthorized commands.

Exfiltration

- Transfer Data to Cloud Account [T1567] – The attacker may attempt to extract sensitive information from the device.

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 industries that rely on Cisco Video Phone 8875 and Cisco Desk Phone 9800 Series for communication, particularly those with high-security and compliance requirements.

- Government
- Energy
- Manufacturing
- Telecommunications
- Utilities
- Education
- Healthcare
- 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 Video Phone 8875 and Desk Phone 9800 Series Information Disclosure Vulnerability