Cisco Webex for BroadWorks Credential Leak – Potential User Impersonation Risk

Overview

Cisco has identified a credential exposure vulnerability in Webex for BroadWorks (Release 45.2) that could allow an unauthenticated, remote attacker to access sensitive data if unsecure transport is configured for SIP communication.

A configuration change has been deployed to mitigate this issue, and customers are advised to restart their Cisco Webex applications to apply the fix.

Affected Products

- **Vulnerable** – Cisco Webex for BroadWorks running in a Windows environment (both on-premises and hybrid cloud/on-premises)
- **Not Vulnerable** – Webex for BroadWorks running in non-Windows environments and Webex for BroadWorks releases earlier than 45.2

This vulnerability stems from the exposure of sensitive credentials in SIP headers and their storage in plain text within client and server logs. If unsecure transport is configured for SIP communication, an unauthenticated attacker could remotely access this information, potentially compromising user accounts.

Additionally, an authenticated user could retrieve credentials from logs, increasing the risk of unauthorized access and impersonation. The issue primarily affects deployments running in Windows environments, including both on-premise and hybrid cloud/on-premises instances of Webex for BroadWorks. See below for workarounds.

Aspire Protects

- Restart Cisco Webex applications to apply the configuration changes.
    - Configure **secure transport for SIP communication** to encrypt data in transit and prevent unauthorized access.
    - This workaround has been tested successfully, but organizations should assess its suitability for their specific environments before implementation.
    - Workarounds or mitigations may affect network performance based on deployment scenarios; administrators should evaluate potential impacts before applying them.
    - Customers should not implement any workaround without first considering its applicability and any possible disruptions to their environment.

- Rotate credentials to prevent potential unauthorized access.
- Assess and validate the workaround before deploying it in a production environment.
- See Cisco's advisory for more information.

TTPs to Watch

Credential Access

- Exploit Public-Facing Application [T1190] – Attackers may attempt to exploit exposed credentials due to unsecure transport configuration.

Privilege Escalation

- Abuse Elevation Control Mechanism [T1548] – Malicious actors could leverage obtained credentials to escalate privileges within affected systems.

IoCs

Targeted Industries

This Cisco vulnerability can impact any industry that relies on Cisco Webex for communications. The vulnerability may impact the following industries/sectors:

- Finance
- Healthcare
- Government
- Manufacturing
- Retail
- Energy
- Education
- 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 Webex for BroadWorks Credential Exposure Vulnerability