Maximum Severity Command Injection Vulnerability Found in Cisco UWRB Access Points

Overview

Cisco has disclosed a critical command injection vulnerability in the Unified Industrial Wireless Software's web-based management interface, affecting Ultra-Reliable Wireless Backhaul (URWB) Access Points. This flaw, tracked as CVE-2024-20418 (CVSS 10), could allow unauthenticated attackers to execute arbitrary commands with root privileges.

CVE-2024-20418 impacts Cisco's Catalyst IW9165D, Catalyst IW9165E, and Catalyst IW9167E Access Points, provided they run vulnerable software versions and/or have URWB operating mode enabled. Other Cisco products, including the Aironet series and Catalyst 9100 Series, are unaffected.

If left unpatched, this vulnerability could give attackers root access to critical Cisco access points, allowing them to control, disrupt, or monitor industrial networks. This could lead to operational downtime and data theft. Cisco advises all customers to review device compatibility and memory requirements before patching.

Aspire Protects

- **Patch –** No workaround exists. Aspire recommends that organizations follow Cisco's patch guidance which can be found in the company's advisory.
- To confirm vulnerability
    - Run the command "show mpls-config". If the command is available, URWB mode is active, indicating the device is at risk.
- Restrict Network Access - Limit access to the management interface to trusted IP ranges only, reducing the risk of unauthorized connections.

IoCs

- There are no known IoCs associated with CVE-2024-20418 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.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application (T1190) – Attackers exploit the web interface via crafted HTTP requests.

Execution

- Command and Scripting Interpreter (T1059) – Arbitrary command execution on the device, enabling attackers to control operations.

Privilege Escalation

- Abuse Elevation Control Mechanism (T1548) – Exploiting the vulnerability for root-level privileges on the device.

Persistence

- Boot or Logon Autostart Execution (T1547*)* – Attackers might modify configurations to establish long-term access on compromised systems.

Collection

- Input Capture (T1056) – Potential capture of sensitive information by monitoring network traffic from compromised devices.

Impact

- Network Denial of Service (T1498) – Attackers could disrupt network availability, impacting industrial operations.

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 cyberattacks.
- **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 Unified Industrial Wireless Software for Ultra-Reliable Wireless Backhaul Access Point Command Injection Vulnerability