Multiple Cisco Vulnerabilities

Overview

Several vulnerabilities have been found in Cisco products that could allow attackers to compromise system security and expose sensitive information. The affected systems include Cisco UCS Central Software, Cisco ATA 190 Series Analog Telephone Adapter firmware, and Cisco Unified Contact Center Management Portal (CCMP).

These vulnerabilities range in severity and can result in unauthorized access, information disclosure, cross-site scripting (XSS) attacks, and system compromise. Cisco has released updates for the affected products, and the vulnerabilities are as follows:

1. **Cisco UCS Central Software Configuration Backup Information Disclosure CVE-2024-20280**
   This vulnerability stems from weak encryption in the backup function of Cisco UCS Central Software, potentially exposing sensitive data like user credentials, SNMP community names, and SSL certificates.
   CVSS Score: 6.3
   Impact: Information disclosure due to static encryption key.
   Affected Products: Cisco UCS Central Software
   Workarounds: None.
   Fixed Release: 2.0(1v) and later.
2. **Cisco ATA 190 Series Analog Telephone Adapter Vulnerabilities**
   Multiple vulnerabilities have been found in the Cisco ATA 190 Series firmware, impacting both on-premises and multiplatform models:
   - **CVE-2024-20458**: Allows an attacker to view or delete device configuration due to lack of authentication on certain HTTP endpoints.
     CVSS Score: 8.2
     Impact: Unauthorized configuration changes.
   - **CVE-2024-20421**: Cross-Site Request Forgery (CSRF) vulnerability allowing remote attackers to perform arbitrary actions.
     CVSS Score: 7.1 (High)
     Impact: CSRF attack on affected device.
   - **CVE-2024-20459**: Command injection vulnerability enabling a high-privileged attacker to execute arbitrary commands.
     CVSS Score: 6.5 (Medium)
     Impact: Command injection and privilege escalation.
   - **CVE-2024-20460**: Reflected XSS vulnerability allowing attackers to execute arbitrary scripts.

CVSS Score: 6.1
Impact: XSS attack on web interface.

- **CVE-2024-20463**: Denial of Service (DoS) through malicious HTTP requests.
  CVSS Score: 5.4
  Impact: DoS and system reboot.

  Affected Products: ATA 191 and ATA 192 running vulnerable firmware.
  Workarounds: Disable web interface for ATA 191 (on-premises).
  Fixed Release: Firmware version 12.0.2 (ATA 191) and 11.2.5 (ATA 192).

3. **Cisco Unified Contact Center Management Portal (CCMP) Reflected XSS Vulnerability CVE-2024-20512**
   The web interface of Cisco CCMP is vulnerable to a reflected XSS attack due to improper validation of user inputs. An attacker can exploit this by tricking users into clicking a malicious link, potentially executing arbitrary scripts.
   CVSS Score: 6.1
   Impact: Reflected XSS leading to information disclosure or further attacks.
   Affected Products: Cisco CCMP
   Workarounds: None.
   Fixed Release: Update available from Cisco.

Aspire Protects

- **Apply Patches**: Cisco has provided updates for all affected products. It is strongly recommended to update to the fixed software versions listed in the advisories.
  - **CVE-2024-20280**
  - **CVE-2024-20458**
  - **CVE-2024-20421**
  - **CVE-2024-20459**
  - **CVE-2024-20460**
  - **CVE-2024-20463**
  - **CVE-2024-20512**
- For Cisco ATA 191 on-premises devices, disabling the web interface can mitigate several vulnerabilities. See Cisco's advisory for further details.
- Watch for suspicious activity, particularly any unauthorized configuration changes or unexpected reboots.

IoCs

There are no known IoCs associated with the above vulnerabilities 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

- Phishing: Spearphishing Link (T1566.002) – Attackers may trick an authenticated user into clicking a specially crafted link to exploit the vulnerability and gain access to the system.

Execution

- Command and Scripting Interpreter: Command Injection (T1059) – Attackers may exploit command injection vulnerabilities in the Cisco ATA firmware to execute arbitrary commands.

Persistence

- Valid Accounts: Exploiting Weak Backup Encryption (T1078.004) – Attackers may use leaked credentials from improperly encrypted backup files in Cisco UCS Central to maintain persistence in the system.

Privilege Escalation

- Exploitation for Privilege Escalation (T1068) – Exploiting the command injection vulnerability in ATA devices to elevate privileges and gain control over the system.

Collection

- Data from Information Repositories (T1213) – Attackers may collect sensitive data such as SNMP community names or user credentials from vulnerable backup files in UCS Central.

Aspire's 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 Managed Security Services**

- Aspire Managed Security Services provide remote security monitoring and device management – 24 hours a day, 7 days a week. By aggregating and correlating security events from across your IT environment, our remote security monitoring service eliminates “noise” and make sense of what really matters.
- Our managed security portfolio includes:
  - Managed Firewall
  - Managed IDS/IPS
  - Security event monitoring & incident management
  - Managed Cisco ISE (Identity Services Engine)
  - Endpoint Protection

Supporting Documentation

Cisco Unified Contact Center Management Portal Reflected Cross-Site Scripting Vulnerability

Cisco UCS Central Software Configuration Backup Information Disclosure Vulnerability

Cisco ATA 190 Series Analog Telephone Adapter Firmware Vulnerabilities