مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in Versa Concerto

Tracking #:432317301

Date:23-05-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed three critical security vulnerabilities have identified in Versa Networks' Concerto orchestration platform that could allow remote attackers to bypass authentication, escape Docker containers, and execute arbitrary code on the host system.

TECHNICAL DETAILS:

Three critical security vulnerabilities have identified in Versa Networks' Concerto orchestration platform that could allow remote attackers to bypass authentication, escape Docker containers, and execute arbitrary code on the host system.

Vulnerability Details

1. **CVE-2025-34026 – Authentication Bypass via Misconfigured Traefik (Spring Boot Heap Dump Access)**
   - **CVSS Score:** 9.2 (Critical)
   - **Type:** Authentication Bypass
   - **Impact:** Allows unauthorized access to internal Spring Boot Actuator endpoints, potentially exposing sensitive memory (heap dumps and trace logs).
   - **Chaining Opportunity:** Can be linked with CVE-2024-45410 for deeper exploitation.

2. **CVE-2025-34027 – Authentication Bypass Leading to RCE via Arbitrary File Write**
   - **CVSS Score:** 10.0 (Critical)
   - **Type:** Authentication Bypass / Remote Code Execution
   - **Impact:** Attackers can upload malicious shared objects and exploit a race condition to overwrite /etc/ld.so.preload, leading to execution of a reverse shell via LD_PRELOAD.
   - **Method:** Abuse of the /portalapi/v1/package/spack/upload endpoint.

3. **CVE-2025-34025 – Docker Escape via Unsafe Mounting**
   - **CVSS Score:** 8.6 (High)
   - **Type:** Privilege Escalation / Container Escape
   - **Impact:** Unsafe default mounting of host binary paths allows attackers to escape the Docker environment and execute code on the underlying host system.
   - **Exploitation:** Attackers can escalate from container access to full host control.

- **Patched versions**: Concerto version 12.2.1 GA or later
- **Mitigations (for unpatched systems)**
  - **Block semicolons (;) in URL paths** to prevent injection.
  - **Drop requests** where the Connection header contains X-Real-Ip.
  - **Restrict access** to the Traefik reverse proxy and administrative endpoints.
  - **Monitor logs** and network traffic for suspicious activity targeting:
    - /portalapi/v1/package/spack/upload
    - /actuator/heapdump and /actuator/trace
  - Implement **Web Application Firewall (WAF)** rules to block anomalous traffic patterns.

RECOMMENDATIONS:

- Upgrade Concerto to fixed patched version or later.
- Apply Mitigations for unpatched systems.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://nvd.nist.gov/vuln/detail/CVE-2025-34026
- https://nvd.nist.gov/vuln/detail/CVE-2025-34027
- https://nvd.nist.gov/vuln/detail/CVE-2025-34025