January 28, 2025

CVE-2025-23006 Overview

Description: A pre-authentication deserialization of untrusted data vulnerability in the SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC) could allow a remote unauthenticated attacker to execute arbitrary OS commands.

CVSS Score: 9.8 (Critical)

Impact:

- Confidentiality: High
- Integrity: High
- Availability: High
- Attack Complexity: Low
- Privileges Required: None
- User Interaction: None

Affected Versions: SMA1000 versions 12.4.3-02804 and earlier.

Exploitation: Threat actors may exploit this vulnerability to execute arbitrary commands on the affected systems.

Recommendation:

- Users should upgrade to version 12.4.3-02854 or higher.
- For dual-homed appliances, restrict administrative console access (port 8443) to trusted internal networks via the internal interface; user VPN traffic remains unaffected.
- For single-homed appliances, use a firewall to limit administrative console access (port 8443) to trusted internal networks, without affecting user VPN traffic.

Source:

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0002

https://www.sonicwall.com/support/knowledge-base/product-notice-urgent-security-notification-sma-1000/250120090802840

https://www.cve.org/CVERecord?id=CVE-2025-23006