

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

SonicWall SMA 1000 Faces Active Exploitation of Critical Vulnerability

Date of Publication

January 24, 2025

Admiralty Code

A1

TA Number

TA2025018




Summary

First Seen: January 22, 2025

Affected Products: SonicWall SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC)

Impact: SonicWall has addressed a critical zero-day vulnerability in its Secure Mobile Access (SMA) 1000 Series appliances, identified as CVE-2025-23006. This flaw, which has been exploited in the wild, allows remote, unauthenticated attackers to execute arbitrary operating system commands under specific conditions, posing a significant security threat.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-23006	SonicWall SMA1000 Appliances Deserialization Vulnerability	SonicWall SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC)			

Vulnerability Details

#1

SonicWall has addressed a critical zero-day vulnerability, CVE-2025-23006, affecting its Secure Mobile Access (SMA) 1000 Series appliances. Secure Mobile Access (SMA) is a solution designed to provide secure remote access to organizational resources, such as applications, data, and networks, over the internet. It is widely used by large organizations to provide secure VPN access to corporate networks. Alarming, this vulnerability has been actively exploited in the wild.

#2

The flaw stems from a pre-authentication deserialization issue in the SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC). Under specific conditions, this vulnerability could allow a remote attacker, without needing to authenticate, to execute arbitrary operating system commands. Successful exploitation could lead to a full compromise of the affected system, putting sensitive data and critical operations at risk.

#3

SonicWall has clarified that this vulnerability does not impact the SMA 100 series appliances, and no action is required for those devices. However, for the SMA 1000 Series, the company has acted swiftly to release a security update to address the issue. Organizations relying on these devices are strongly encouraged to apply the latest firmware updates immediately to protect against potential exploitation.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-23006	SonicWall SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC) Version 12.4.3-02804 and earlier	cpe:2.3:h:sonicwall:sma1000 *.*.*.*.*.*.*.*	CWE-502

Recommendations



Update: Upgrade to the SonicWall SMA 1000 Series appliances latest version 12.4.3-02854 (platform-hotfix) or higher versions, which contains the patch for CVE-2025-23006. Ensure regular patch management practices are followed to address newly disclosed vulnerabilities.



Secure Management Interface Access: Ensure the SMA Appliance Management Console (AMC) and Central Management Console (CMC) are only accessible from trusted networks. Implement IP whitelisting to allow connections exclusively from authorized devices, reducing the risk of unauthorized access.



Network Segmentation: Isolate SMA 1000 appliances from critical network segments to minimize the risk of lateral movement by attackers in the event of a breach. This containment strategy ensures sensitive systems and data remain protected, even if the appliance is compromised.



Secure Administrative Access to SMA & CMS: It is recommended that users restrict administrative access to their SMA and Central Management Server (CMS) appliances. For dual-homed appliances, limit access to the administrative console (default TCP port 8443) to trusted internal networks via an internal interface, which won't interfere with user VPN traffic. For single-homed appliances, configure a firewall to restrict access to the administrative console to trusted internal networks, also ensuring that user VPN traffic remains unaffected.

Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>T1588</u> Obtain Capabilities
<u>T1588.006</u> Vulnerabilities	<u>T1190</u> Exploit Public-Facing Application	<u>T1059</u> Command and Scripting Interpreter	

Patch Details

Promptly update to the latest version of SonicWall SMA1000 devices to Version 12.4.3-02854 (platform-hotfix) or higher, this version includes the necessary patch to address the vulnerability.

Link:

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

References

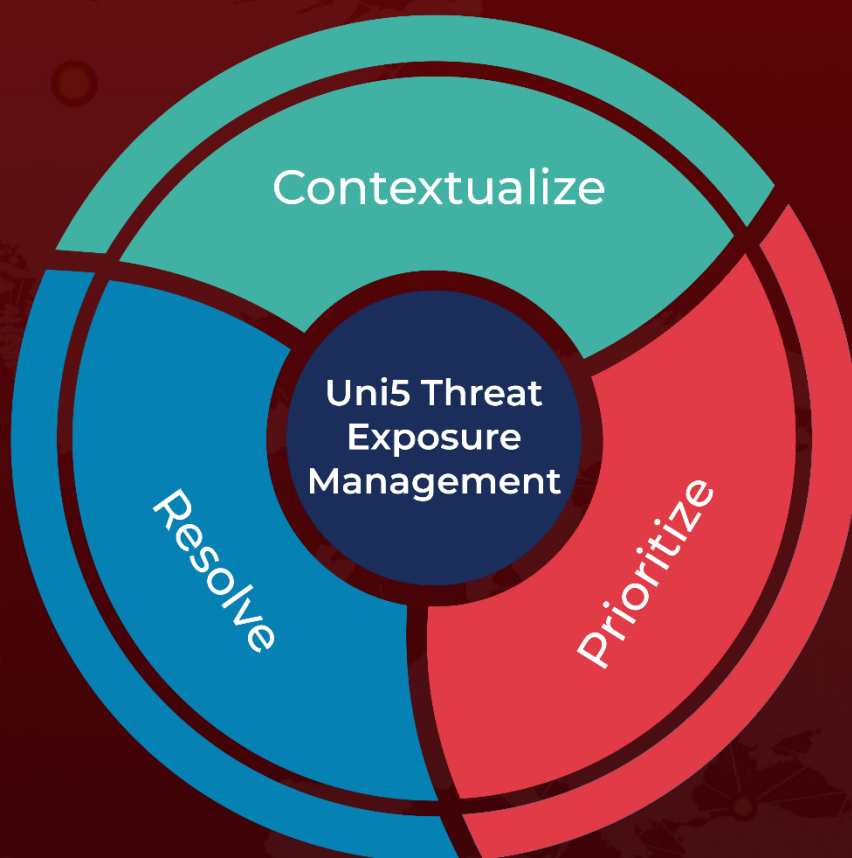
<https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0002>

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

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

January 24, 2025 • 5:45 AM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com