Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Urgent Patch Required: Active Attacks Exploiting SonicWall SMA Vulnerabilities

Date of Publication	Admiralty Code	TA Number
May 2, 2025	A1	TA2025134

Summary

First Seen: December 2023
Affected Products: SMA100 SSL-VPN
Impact: SonicWall has confirmed that attackers are actively exploiting two vulnerabilities CVE-2023-44221 and CVE-2024-38475 affecting SMA 100 Series appliances. These flaws can allow authenticated attackers to inject system commands and let unauthorized users hijack sessions by accessing sensitive files. If left unpatched, they could lead to full device compromise. Organizations using SMA should urgently update to the latest firmware and review device logs for any signs of unauthorized access.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-38475	Apache HTTP Server Improper Escaping of Output Vulnerability	SMA100 SSL-VPN	✗	✓	✓
CVE-2023-44221	SonicWall SMA100 Appliances OS Command Injection Vulnerability	SMA100 SSL-VPN	✗	✓	✓

Vulnerability Details

#1 SonicWall has confirmed that two security vulnerabilities, CVE-2023-44221 and CVE-2024-38475, have been actively exploited in real-world attacks targeting its SMA 100 Series Secure Mobile Access appliances.

#2 CVE-2024-38475 impacts SonicWall SMA devices, specifically models 200, 210, 400, 410, and 500v. This flaw stems from improper handling of output in the mod_rewrite module of the Apache HTTP Server (version 2.4.59 and earlier), which these devices rely on. Exploiting this bug could allow attackers to map crafted URLs to sensitive file paths on the system. In some cases, this can open the door to unauthorized access and even session hijacking.

#3 Meanwhile, CVE-2023-44221 is an OS command injection vulnerability in the SMA100 SSL-VPN management interface. It allows an attacker who already has administrative access to inject arbitrary system commands. These commands are executed as the 'nobody' user, potentially giving attackers a way to run malicious code on the underlying operating system.

#4 To protect your environment, it's essential to immediately apply the latest security updates for all affected SMA devices. You should also audit your logs for unusual or unauthorized login activity to catch any signs of compromise early. Staying current with patches is the best defense against these known, actively exploited threats.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-38475	SMA 100 Series (SMA 200, 210, 400, 410, 500v) Version 10.2.1.13-72sv and earlier versions	cpe:2.3:o:sonicwall:sma_firmware:*:*:*:*:*:*:*:*	CWE-116
CVE-2023-44221	SMA 100 Series (SMA 200, 210, 400, 410, 500v) Version 10.2.1.9-57sv and earlier versions	cpe:2.3:o:sonicwall:sma_firmware:*:*:*:*:*:*:*:*	CWE-78

Recommendations

Update Immediately: Apply the latest security patches provided by SonicWall to address both vulnerabilities. Delaying updates leaves systems open to active exploitation.

Review Access Logs: Check your SMA device logs for any signs of unauthorized access or suspicious activity, especially from unknown IP addresses or unusual login times.

Restrict Management Access: Limit access to the management interface to trusted internal networks or via a secure VPN. Avoid exposing it directly to the internet whenever possible.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0007** Discovery
T1588 Obtain Capabilities	**T1588.006** Vulnerabilities	**T1059** Command and Scripting Interpreter	**T1078** Valid Accounts
T1190 Exploit Public-Facing Application	**T1083** File and Directory Discovery		

Patch Details

Update your SMA Devices to the latest version to address the Flaws.
For CVE-2023-44221: Upgrade to Version 10.2.1.10-62sv and higher.
For CVE-2024-38475: Upgrade to Version 10.2.1.14-75sv and higher.

Links:
https://httpd.apache.org/download.cgi ,
https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0018

References

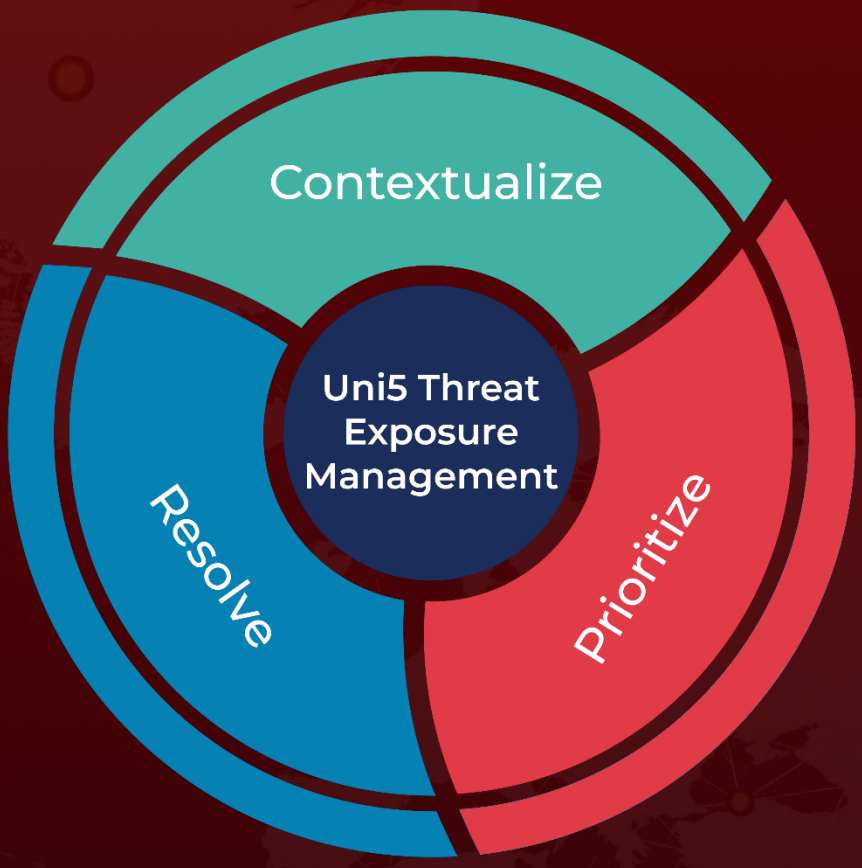
https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0018

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0018

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

May 2, 2025 • 4:50 AM

More at www.hivepro.com