Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Two SMA 1000 Zero-Days Open SonicWall Appliances to RCE

Date of Publication	Admiralty Code	TA Number
September 04, 2026	A1	TA2026255

Summary

First Seen: September 2026
Affected Products: SonicWall SMA 1000 series
Impact: SonicWall has confirmed that attackers are actively exploiting two newly disclosed zero-day vulnerabilities in its Secure Mobile Access (SMA) 1000 series appliances. The first flaw, CVE-2026-83548, is a maximum-severity pre-authentication server-side request forgery (SSRF) weakness in the appliance's Work Place interface that lets an unauthenticated attacker reach sensitive internal functionality. The second, CVE-2026-83549, is an operating system command injection flaw in the Appliance Management Console (AMC) that an administrator-level attacker can use to run arbitrary commands on the device. SonicWall discovered the issues internally, has released hotfixes, and is urging every customer to patch without delay.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-83548	SonicWall SMA1000 Appliances Server-Side Request Forgery Vulnerability	SonicWall SMA 1000	✓	✓	✓
CVE-2026-83549	SonicWall SMA1000 Appliances OS Command Injection Vulnerability	SonicWall SMA 1000	✓	✓	✓

Vulnerability Details

#1

SonicWall has issued security updates for two vulnerabilities in its Secure Mobile Access (SMA) 1000 series VPN appliances that attackers have already been exploiting as zero-days. The flaws sit in different components of the SMA 1000 but combine into a single powerful attack path. CVE-2026-83548 is classified as a server-side request forgery issue (CWE-918) in the Appliance Work Place interface, the user-facing portal exposed to the internet. Because it can be triggered before any authentication, a remote attacker can abuse the appliance to make requests on their behalf and reach functionality that should never be accessible from outside.

#2

CVE-2026-83549 is an operating system command injection flaw (CWE-78) in the Appliance Management Console, the administrative back end of the device. Under specific conditions, an attacker operating with administrator privileges can inject and execute arbitrary OS commands, which translates directly into remote code execution on the underlying system. On their own, each flaw carries a distinct risk: one exposes internal functions to unauthenticated attackers, and the other allows an administrator to execute arbitrary commands on the appliance. Considered together, though, the two flaws carry a high potential for chaining: pairing a pre-authentication weakness with a code-execution flaw is exactly the kind of combination attackers seek to link, which could let them progress from an unauthenticated foothold toward full control of the appliance.

#3

The flaws affect both physical and virtual SMA 1000 models, specifically the 6210, 7210, and 8200v, running firmware 12.4.3-03453 (platform-hotfix) and 12.5.0-02835 (platform-hotfix) or earlier. Importantly, the SMA 100 series and SonicWall's firewall SSL-VPN offerings are not affected, which narrows the exposure to organizations specifically running SMA 1000 hardware or virtual appliances.

#4

SonicWall's Product Security Incident Response Team confirmed it investigated a case pointing to active exploitation of these vulnerabilities. Because attacks are already underway against internet-facing appliances, applying the available hotfix immediately is essential; every day an unpatched SMA 1000 stays online is a day it can be targeted with a flaw that is being exploited right now.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-83548	SonicWall SMA 1000 (6210, 7210, 8200v) 12.4.3-03453 and 12.5.0-02835 (platform-hotfix) and older versions	cpe:2.3:a:sonicwall:sma1000:*:*:*:*:*:*:*:*	CWE-918, CWE-441
CVE-2026-83549	SonicWall SMA 1000 (6210, 7210, 8200v) 12.4.3-03453 and 12.5.0-02835 (platform-hotfix) and older versions	cpe:2.3:a:sonicwall:sma1000:*:*:*:*:*:*:*:*	CWE-78

Recommendations

Apply the SonicWall Hotfix Immediately: Upgrade every SMA 1000 appliance to the fixed firmware, version 12.4.3-03526 (platform-hotfix) or 12.5.0-02952 (platform-hotfix), as soon as possible. With attacks already underway and a CVSS 10.0 flaw in play, patching is the single most effective step and should take priority over routine maintenance windows.

Rebuild and Reset After a Confirmed Breach: If you find evidence of compromise, re-image physical appliances or re-deploy virtual ones from a known-good state, then change all user and administrator passwords and reset every Time-based One-Time Password (TOTP) token. Patching alone does not remove an attacker who already gained access, so a full reset is essential.

Reduce Exposure at the Network Edge: Limit who can reach the SMA 1000 management interfaces by restricting administrative access to trusted networks and, where possible, placing the appliance behind additional access controls. Shrinking the internet-facing attack surface buys time and lowers the chance of opportunistic exploitation.

Strengthen Vulnerability Management: Maintain an accurate inventory of edge and remote-access devices, monitor vendor advisories closely, and build a process to test and deploy security hotfixes quickly. Edge appliances like the SMA 1000 are repeatedly targeted, so treating them as high-priority assets in your patching program pays off over time.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Patch Link

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0016

References

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0016

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 Demo of **HivePro**.

REPORT GENERATED ON

September 04, 2026 • 12:30 AM

More at www.hivepro.com