Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

SonicWall SMA1000 Zero-Days Under Active Exploitation

Date of Publication	Admiralty Code	TA Number
July 16, 2026	A1	TA2026201

Summary

First Seen: July 2026
Affected Products: SonicWall SMA1000 Series (models 6210, 7210, and 8200v)
Impact: SonicWall has warned that attackers are actively exploiting two zero-day flaws in its SMA1000 Series remote access appliances. The first, CVE-2026-15409, is a critical flaw (CVSS 10.0) that lets an attacker with no login reach services that are meant to stay hidden inside the appliance. The second, CVE-2026-15410, then lets them run their own commands as the top-level "root" user, which means full control of the device. Both vulnerabilities are confirmed as actively exploited, and because there are no workarounds, organizations running affected appliances should treat patching and forensic review as an emergency.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-15409	SonicWall SMA1000 Appliances Server-Side Request Forgery Vulnerability	SonicWall SMA1000	✓	✓	✓
CVE-2026-15410	SonicWall SMA1000 Appliances Code Injection Vulnerability	SonicWall SMA1000	✓	✓	✓

Vulnerability Details

#1

SonicWall has warned of active exploitation of two zero-day vulnerabilities impacting its Secure Mobile Access (SMA) 1000 Series appliances. The first and most severe, CVE-2026-15409, is a server-side request forgery weakness (CWE-918) in the SMA1000 WorkPlace application. The problem lives in a websocket proxy feature reachable at the /wsproxy path. This feature works like a netcat-style TCP tunnel and takes the target host and port directly from user-supplied URL parameters. By pointing those parameters at the loopback address, an unauthenticated attacker can send and receive raw TCP traffic to and from services that are only meant to be reachable locally on the appliance.

#2

That local reach is what makes the flaw so dangerous. Once inside the loopback boundary, an attacker can talk to less-hardened internal services, such as an Erlang process on port 1050 or the ctrl-service application on port 8188. In testing, researchers reached the Erlang service and achieved code execution using a hardcoded cookie value, meaning authentication was not actually required to run commands. This is the first-stage foothold that was observed being exploited in the wild.

#3

The second flaw, CVE-2026-15410, is an improper control of code generation issue (CWE-94) in the Appliance Management Console. It is a path traversal in the remove_hotfix workflow for ctrl-service, accessible via the web console. An attacker supplies a hotfix value containing a traversal sequence that points to a malicious script they have already staged on the device. The system then makes the script executable and runs it as root before rebooting the appliance. If the referenced file does not exist, no reboot happens; if it does exist, the appliance chmods and executes it under UID 0. This turns the earlier low-privileged code execution into full root control.

#4

The two vulnerabilities give an unauthenticated remote attacker a clean path from the public internet to root on the appliance. The impact is limited to the SMA1000 Series; SonicWall has confirmed these issues do not affect SSL VPN functionality on SonicWall firewalls or the SMA 100 Series product line. The affected software covers SMA1000 Series models 6210, 7210, and 8200v running builds 12.4.3-03245, 12.4.3-03387, and 12.4.3-03434, as well as 12.5.0-02283, 12.5.0-02624, and 12.5.0-02800. A public proof-of-concept for CVE-2026-15409 already exists, and a Metasploit module for the full chain is reportedly in development, so exploitation is expected to broaden quickly.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-15409	SonicWall SMA1000 Series 6210, 7210, 8200v 12.4.3-03245, 12.4.3-03387 and 12.4.3-03434 (platform-hotfix) 12.5.0-02283, 12.5.0-02624 and 12.5.0-02800 (platform-hotfix)	cpe:2.3:a:sonicwall:sma1000:*:*:*:*:*:*:*:* cpe:2.3:o:sonicwall:sma6210_firmware:*:*:*:*:*:*:*:* cpe:2.3:o:sonicwall:sma7210_firmware:*:*:*:*:*:*:*:* cpe:2.3:a:sonicwall:sma8200v:*:*:*:*:*:*:*:*	CWE-918
CVE-2026-15410			CWE-94

Recommendations

Patch on an Emergency Basis: Upgrade affected SMA1000 appliances to the fixed platform-hotfix releases without delay. SonicWall has published fixes in version 12.4.3-03453 (or later) and 12.5.0-02835 (or later) for the 6210, 7210, and 8200v models. Because active exploitation is confirmed and there are no workarounds, patching is the single most important step and should be scheduled as an emergency change.

Hunt for Compromise Before Trusting the Appliance: Do not assume a patched device is a clean device. Review appliance logs for the published indicators, including extraweb_access.log entries showing /wsproxy requests that return HTTP 101 with suspicious localhost host parameters, and ctrl-service.log entries showing remove_hotfix invoked with path-traversal sequences pointing at staged shell scripts. Also check for rogue /__api__/login or /__api__/logout routes inside /var/lib/unit/conf.json, which are not present in legitimate configurations.

Rebuild and Rotate if Compromise Is Found: If any indicator of compromise is identified, treat the appliance as fully compromised. Re-image physical appliances or redeploy virtual appliances from a known-good image, change all user and administrator passwords, and reset TOTP tokens, since attackers were observed stealing credentials and MFA seeds for long-term access that survives network-level cleanup.

Watch for Lateral Movement into Active Directory: Look for VPN-less authentications originating from the appliance's internal IP address into domain controllers, especially NTLM logons (Windows Event ID 4624, logon type 3) using atypical workstation names such as "kali" under the appliance's LDAP service account. This pattern was the tell-tale sign that the appliance had become a backdoor into the internal directory.

Reduce Exposure and Restrict Access: Limit or block traffic to and from the FNS Holdings Limited hosting infrastructure (ASN 206092) if there is no business need, since the observed attacks originated from IP space belonging to that VPN provider. More broadly, minimize direct internet exposure of management interfaces and place remote access appliances behind additional network controls where feasible.

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	
Credential Access	T1552: Unsecured Credentials	
Lateral Movement	T1021: Remote Services	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Patch Link

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0008

References

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0008

https://github.com/remmons-r7/rapid7-CVE-2026-15409

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

July 16, 2026 • 09:00 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com