



Hotfixes Released for SonicWall SMA 1000 Series Appliances

Oct 07, 2026

[View Alert](#)

☐ WHITE

SonicWall has issued security [updates](#) to address four vulnerabilities affecting its Secure Mobile Access (SMA) 1000 series appliances, highlighted by a maximum-severity Server-Side Request Forgery (SSRF) flaw tracked as CVE-2026-102255.

Exploitation of this vulnerability allows unauthenticated, remote attackers to bypass access controls and force the appliance to execute unauthorized requests against internal services. While SonicWall reports no active exploitation in the wild at this time, immediate application of official vendor hotfixes is strongly recommended due to high adversary interest in edge remote-access devices.

Health-ISAC provides this information to increase situational awareness and encourage organizations to assess their risk exposure to the vulnerabilities.

Additional Info

Analysis:

SonicWall has disclosed multiple security flaws in its Secure Mobile Access (SMA) 1000 series gateways, led by CVE-2026-102255, a critical Server-Side Request Forgery

vulnerability carrying a maximum severity rating. The root cause stems from an unintended alternate access path flaw in the appliance's user-facing Appliance WorkPlace interface. Alongside this critical flaw, SonicWall patched three additional vulnerabilities, including a post-authentication OS command injection bug (CVE-2026-102256), an authenticated path traversal flaw (CVE-2026-102257), and a cross-site scripting (XSS) vulnerability (CVE-2026-102258) in the Appliance Management Console (AMC).

From an exploitation standpoint, CVE-2026-102255 represents a significant risk because it requires no prior privileges or authentication and exhibits low attack complexity. A remote threat actor can transmit specially crafted HTTP requests directly to the internet-facing Appliance WorkPlace portal, manipulating the gateway into routing requests on the attacker's behalf. By exploiting implicit network trust in the gateway, attackers can access restricted internal endpoints, interact with backend services, and perform administrative operations typically accessible only to authenticated users.

The vulnerabilities affect both hardware and virtual appliances across the SMA 1000 product line running vulnerable firmware builds, including the SMA 6210, SMA 7210, and SMA 8200v. Conversely, SonicWall confirmed that its SMA 100 series appliances and firewall-hosted SSL-VPN deployments are entirely unaffected by these flaws. Organizations deploying impacted SMA 1000 models should prioritize inventory verification, as exposing these gateways to the internet makes them prime targets for edge network discovery and initial access.

Regarding remediation, SonicWall has released official firmware hotfixes to resolve all four flaws; notably, no documented workarounds or mitigation alternatives are available to neutralize the exposure without upgrading. Although the vendor indicates that there is currently no evidence of active in-the-wild exploitation for CVE-2026-102255, SMA 1000 gateways have been repeatedly targeted by advanced threat actors and ransomware affiliates. Given that threat actors have chained similar SMA 1000 flaws in prior zero-day intrusion campaigns, rapid patching is critical before weaponized exploits emerge.

Recommendations and Mitigations:

Health-ISAC recommends organizations review and assess their risk exposure to the vulnerabilities and implement the following:

- Upgrade all SMA 6210, 7210, and 8200v deployments to firmware versions 12.4.3-03670 or 12.5.0-03082 (and higher); no workarounds are available.
- Limit access to the Appliance WorkPlace and Appliance Management Console (AMC) to trusted IP ranges or dedicated management subnets via upstream ACLs.
- Monitor gateway telemetry for abnormal outbound requests originating from the appliance toward internal subnets (RFC 1918 space) or loopback addresses.
- Review internet-facing assets to identify unpatched or improperly exposed SMA 1000 interfaces.
- Review the [Guidance and Strategies to Protect Network Edge Devices](#) resources.
- Review the Health Industry Cybersecurity Practices (HICP): [Managing Threats and Protecting Patients](#) resources.

<hr size=1 width="100%" align=center>

Alert Id cb668d2a

Category Vulnerability Bulletins

References [bleepingcomputer](#) [helpnetsecurity](#) [cisa](#) [sonicwall](#) [hhs](#) [sonicwall](#)
[1](#)

Tags

CVE-2026-102258, CVE-2026-102257, CVE-2026-102256, CVE-2026-102255, SMA 1000, SonicWall

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Please provide your feedback



Download the App

Available on iOS, Android and Web



For more updates and alerts, visit: <https://health-isac.cyware.com/webapp/>

Health-ISAC is an invite only platform. Please DO NOT forward this email to anyone. If you are not supposed to receive this email, please report to toc@h-isac.org