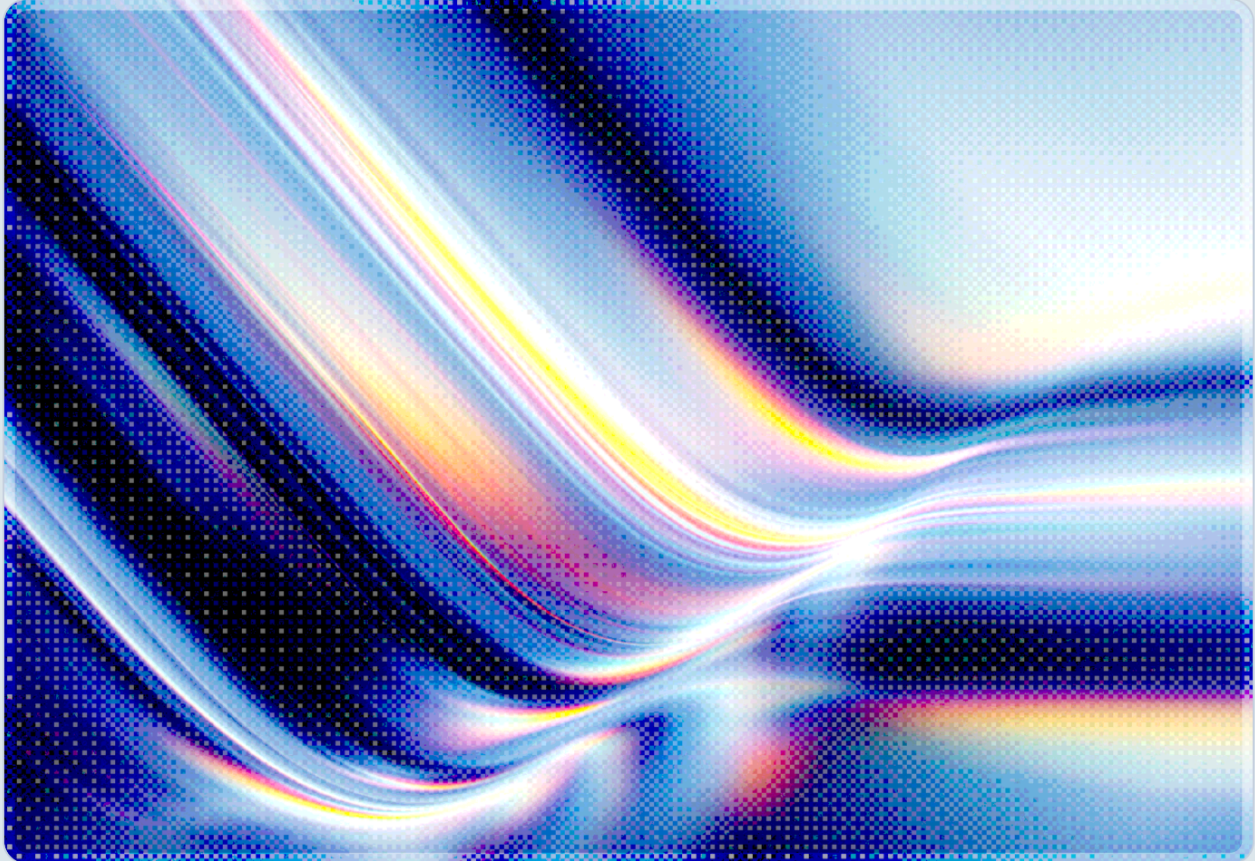


SonicWall SMA 1000: A Third Maximum-Severity SSRF

CVE-2026-102255 and the Recurring Pre-Authentication Flaw Class in the WorkPlace Portal

2026-10-08

 AI-assisted Rapid Research



CSAI

cloud
security
alliance®

© 2026 Cloud Security Alliance. Some rights reserved.

You may download, store, display, view, print, redistribute, and link to this document in its original, unmodified form, provided that attribution to the Cloud Security Alliance is maintained and all trademark and copyright notices remain intact.

This document may not be modified or altered. You may quote portions of the document as permitted by the Fair Use provisions of the United States Copyright Act, provided that attribution is given to the Cloud Security Alliance.

This document may be shared on professional and social media platforms in its original form with attribution.

This document was generated with AI assistance and has not undergone official CSA review and approval processes.

Key Takeaways

SonicWall has patched CVE-2026-102255, a pre-authentication server-side request forgery (SSRF) flaw in the WorkPlace interface of SMA 1000 appliances. SonicWall rates it CVSS 10.0 [2][4], and it is tracked under advisory SNWLID-2026-0017 [1][4]. The weakness stems from what the vendor calls "an unintended alternate access path," which allows an unauthenticated attacker to make the appliance issue requests on the attacker's behalf and reach internal functionality [1][3].

This is the third maximum-severity, pre-authentication SSRF in the same SMA 1000 component between July 14 and October 7, 2026, a span of about twelve weeks. The July 2026 flaw (CVE-2026-15409) was exploited as a zero-day before a patch shipped [6], and SonicWall confirmed active exploitation of the September 2026 flaw (CVE-2026-83548) [5]. As of the sources reviewed, SonicWall reports no evidence that CVE-2026-102255 or the three other flaws fixed in the same release are being exploited [1][2][4].

Because both earlier SSRF flaws were exploited in the wild, and because SonicWall states there is no workaround [4], organizations should treat this patch as an emergency change even without confirmed exploitation. That is a judgment on our part rather than a vendor statement. Internet-facing SMA 1000 appliances on firmware 12.4.3-03526 or earlier, or 12.5.0-02952 or earlier, remain exposed until upgraded [1][2].

Background

The SMA 1000 series is SonicWall's remote-access gateway family, sold as the physical 6210 and 7210 models and the virtual 8200v [1][2]. The appliance exposes a user-facing WorkPlace portal to the internet and a separate Appliance Management Console (AMC) intended to be reachable only by administrators on a protected network segment. This division matters because the appliance typically holds privileged network position, VPN session state, and credentials for the internal directory. A flaw that lets an outside party borrow the appliance's network position therefore carries consequences well beyond the device itself.

CVE-2026-102255 follows two earlier incidents. On July 14, 2026, SonicWall disclosed CVE-2026-15409, a CVSS 10.0 unauthenticated SSRF, together with CVE-2026-15410, a code injection flaw rated CVSS 7.2. Attackers chained the pair to achieve unauthenticated root command execution, and CSA's earlier analysis documented the exploitation chain and the post-exploitation credential and TOTP seed harvesting that followed [6][7]. On September 1, 2026, SonicWall disclosed a second pair: CVE-2026-83548, another CVSS 10.0 pre-authentication SSRF caused by the WorkPlace endpoint acting as an unintended forward proxy to the AMC, and CVE-2026-83549, a post-authentication command execution flaw in the AMC rated 7.8. SonicWall stated that it was actively exploiting both vulnerabilities [5].

The October release, announced on October 7, fixes four vulnerabilities. Alongside the SSRF, it addresses an OS command injection requiring administrator login (CVE-2026-102256, CVSS 7.8), a Zip Slip path traversal in the AMC (CVE-2026-102257, CVSS 7.2), and a stored cross-site scripting flaw in the AMC (CVE-2026-102258, CVSS 5.5) [2]. Help Net Security and The Hacker News credit Benoît Sevens of Anthropic with CVE-2026-102255 and CVE-2026-102256, and Brian Mariani of DigitalCanion SA with the other two [1][2], while the Truesec and Security Affairs articles reviewed do not name researchers [3][4].

Security Analysis

The vulnerability and affected versions

The reported technical detail is limited, and SonicWall has not published an exploit description. The public statements establish that the WorkPlace interface exposes a path to internal functionality that was not meant to be reachable by unauthenticated users, and that the appliance can be induced to issue requests that internal endpoints trust [1][3]. We cannot confirm from these sources which internal endpoint is reachable or what requests an attacker would send. The table below summarizes what is reported.

Item	Reported detail	Source
CVE / advisory	CVE-2026-102255 / SNWLID-2026-0017	[1][4]
Type	Pre-authentication SSRF (CWE-918) in WorkPlace interface	[1][3]
Severity	CVSS 10.0 (vendor score)	[2][4]

Item	Reported detail	Source
Affected models	SMA 1000 6210, 7210, 8200v	[1][2]
Vulnerable builds	12.4.3-03526 and earlier; 12.5.0-02952 and earlier	[1][2]
Fixed builds	12.4.3-03670 and later; 12.5.0-03082 and later	[1][2]
Workaround	None reported; hotfix via MySonicWall portal	[2][4]
Exploitation	No evidence in the wild at time of reporting	[1][2][4]

A recurring flaw class, not an isolated bug

The three maximum-severity flaws share a component, an authentication level, and a bug class. Each is a pre-authentication SSRF in the WorkPlace interface of the same SMA 1000 product family, and each scored 10.0 [2][5][6]. The descriptions of the root cause are also similar in kind: an "unintended forward-proxy function" in September and an "unintended alternate access path" in October [1][5]. We infer from this that the WorkPlace code may have request-routing behavior that is hard to constrain, and that earlier fixes closed individual paths without removing the underlying exposure. That is an inference from the pattern in vendor descriptions, not a finding from SonicWall or any cited researcher.

The pattern also suggests how this flaw may be used. In both prior incidents the SSRF served as the unauthenticated stepping stone, and a second flaw in an administrator-only component supplied code execution [5][6]. The October release contains an administrator-gated command injection (CVE-2026-102256) and an AMC path traversal (CVE-2026-102257) [2], which fits the same structure. No source reviewed demonstrates that these flaws can be chained, so this should be read as a plausible attack path that defenders should anticipate. It is not a reported exploit chain.

Why exploitation risk is elevated despite no reported attacks

SonicWall and the press coverage state that no exploitation is currently known [1][2][4]. The absence of known exploitation is a weak signal for this product family, given that the earlier flaws were exploited in the wild. The July flaws were exploited before disclosure, with CSA's analysis noting activity from multiple independent actors, including a ransomware affiliate [6]. SonicWall stated that it was actively exploiting both September flaws [5], although the source we reviewed does not say whether that exploitation preceded the patch. Help Net Security describes these devices as regularly targeted and

recalls the two earlier pre-authentication SSRF zero-days [1]; we consider the risk elevated for that reason. Patch diffing is a common technique, and we expect exploit development to be feasible once a fix is public, though we have no data specific to this CVE.

Post-compromise consequences

If an attacker reaches the AMC or achieves code execution, the earlier incidents show what follows. CSA's July analysis describes harvesting of administrator credentials, session databases, and TOTP seeds, then authentication into internal Active Directory directly rather than through the VPN tunnel [6]. In the July incidents, where TOTP seeds were stolen from the appliance, multi-factor authentication offered little protection [6]. The same analysis concluded that patching alone does not remediate an appliance that was compromised before the patch, which is why compromise assessment belongs alongside patching [6][7].

Relevance to AI-adjacent infrastructure

This note concerns a network appliance rather than an AI system, but the exposure is relevant to AI programs. Remote-access gateways commonly front the internal networks where model training environments, inference services, and agent tooling are hosted. A compromised gateway offers an attacker a path into those environments with the trust of a legitimate remote user. Organizations that route privileged AI development or operations access through an SMA 1000 should include that dependency in their risk assessments.

Recommendations

Immediate Actions

Identify every SMA 1000 appliance, including virtual 8200v instances and any managed through a central management server, and compare build numbers against the vulnerable ranges above. Apply the hotfix from the MySonicWall portal to reach 12.4.3-03670 or 12.5.0-03082 or later; the appliance restarts after installation, so schedule the change accordingly [2]. Because no workaround exists, restricting exposure is not a substitute for patching, although limiting the WorkPlace portal to required source networks, where the business allows it, reduces the population of potential attackers. Confirm the patch status of the September 1 hotfixes as well, since appliances that skipped that release may have been exposed to an exploited flaw [5].

Review the appliances for signs of earlier compromise rather than assuming a clean history. CSA's July analysis identifies the logs and request patterns worth examining for the earlier SSRF, and the same review should look for unexpected requests to the AMC from the WorkPlace interface [6]. If indicators are present, treat the appliance as compromised, redeploy it from a clean image, and rotate administrator and user credentials and reissue TOTP seeds [6].

Short-Term Mitigations

Reduce what a compromised appliance can reach. Review the internal network paths the SMA 1000 can access and remove those not needed for current access policy, and confirm the AMC is on a management segment that is not reachable from user-facing interfaces or the internet. Audit Active Directory authentication logs for sign-ins attributed to the appliance's service identity from unexpected hosts or times, which is the lateral movement pattern documented in July [6]. Add the SonicWall PSIRT advisory feed to the vulnerability intake process, and monitor CISA's Known Exploited Vulnerabilities catalog for this CVE, since the sources reviewed do not report a listing.

Strategic Considerations

Three maximum-severity flaws in one component in about twelve weeks raises a governance question that goes beyond patch speed: whether the residual risk of an internet-exposed SSL-VPN gateway is acceptable for the data it protects. CSA's earlier analysis argued for identity-centric, software-defined perimeter architectures in which the gateway has narrower reach and users authenticate before network connectivity is granted [6]. Organizations should evaluate whether SMA 1000 workloads can move to such a model, and in the interim should track vendor flaw recurrence as an input into vendor risk reviews. Contract and procurement teams may also reasonably ask SonicWall what code-level changes address the underlying request-handling design, since the public advisories describe each fix as closing an unintended path.

CSA Resource Alignment

CSA has published several rapid-research notes on earlier SMA 1000 incidents, and they are the most directly relevant prior work. *SonicWall SMA Zero-Days: Edge Appliance Root Returns* [6] documents the July 2026 SSRF and code-injection chain, the credential and TOTP seed theft that followed, and the forensic review steps. The compromise-assessment and credential-reset guidance in this note builds on that analysis, and the earlier note's argument for reducing appliance blast radius applies directly to CVE-

2026-102255. *SonicWall SMA1000 Zero-Days: Patch Before the Federal Deadline* [7] covers the same July flaws from the remediation-deadline perspective and is useful for organizations establishing patch-timing expectations for this product family.

UTA0533: Weeks-Long Espionage Chain in SonicWall SMA1000 [8] examines extended pre-disclosure exploitation of the July flaws, which supports the caution in this note that the absence of reported exploitation should not delay patching. As a standing framework, the AI Controls Matrix (AICM) v1.1 [9] addresses these findings through its Threat and Vulnerability Management and Identity and Access Management domains, covering vulnerability remediation timelines, credential hygiene, and access segmentation for infrastructure that supports AI workloads.

References

- [1] Help Net Security. "[SonicWall fixes pre-auth SSRF flaw in SMA 1000 appliances \(CVE-2026-102255\)](#)." Help Net Security, October 7, 2026.
- [2] The Hacker News. "[SonicWall Patches CVSS 10.0 Pre-Authentication SSRF Flaw in SMA1000 Appliances](#)." The Hacker News, October 2026.
- [3] Truesec. "[Critical SonicWall SMA1000 Pre-Authentication SSRF Vulnerability](#)." Truesec, October 2026.
- [4] Security Affairs. "[SonicWall Fixes Max Severity Pre-Auth Flaw in SMA1000 Appliances](#)." Security Affairs, October 2026.
- [5] Security Affairs. "[SonicWall Patches Two New Actively Exploited Zero-Days in SMA 1000 VPNs](#)." Security Affairs, September 2, 2026.
- [6] Cloud Security Alliance. "[SonicWall SMA Zero-Days: Edge Appliance Root Returns](#)." CSA AI Safety Initiative, July 20, 2026.
- [7] Cloud Security Alliance. "[SonicWall SMA1000 Zero-Days: Patch Before the Federal Deadline](#)." CSA AI Safety Initiative, July 15, 2026.
- [8] Cloud Security Alliance. "[UTA0533: Weeks-Long Espionage Chain in SonicWall SMA1000](#)." CSA AI Safety Initiative, July 25, 2026.
- [9] Cloud Security Alliance. "[AI Controls Matrix v1.1](#)." Cloud Security Alliance, 2026.