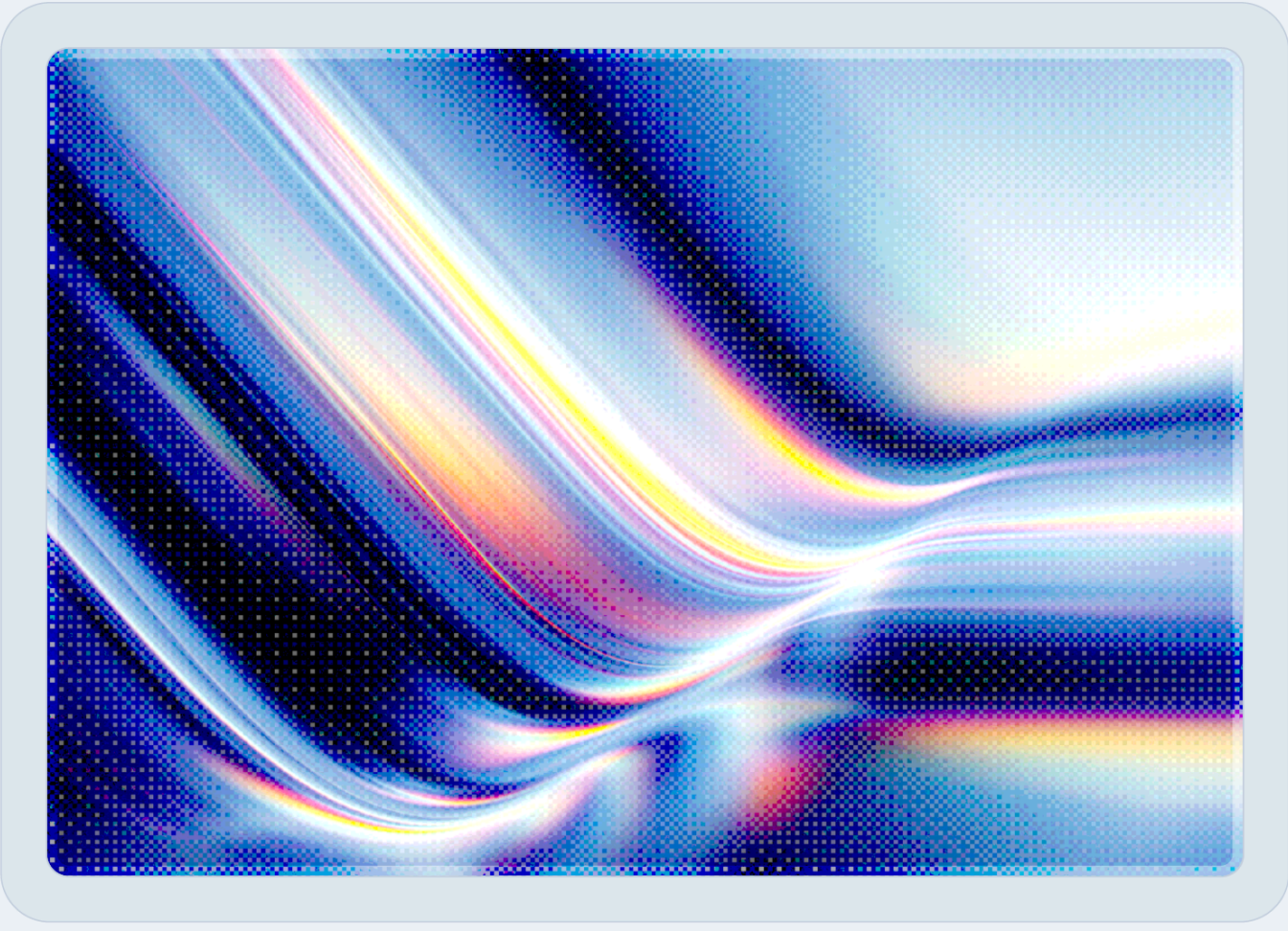
CSAI Foundation | Cloud Security Alliance

SonicWall SMA Zero-Days: Edge Appliance Root Returns

Chained SSRF and Code Injection Flaws in SMA 1000 Enable Unauthenticated Root Compromise

2026-07-20

AI-assisted Rapid Research



CSAI | CSA cloud security alliance®

Key Takeaways

- SonicWall disclosed two zero-day vulnerabilities in its SMA 1000 series remote-access appliances — CVE-2026-15409, an unauthenticated server-side request forgery (SSRF) scored CVSS 10.0, and CVE-2026-15410, a code injection flaw scored CVSS 7.2 that relies on the internal-only access the SSRF already provides rather than valid login credentials (CISA classifies it "post-authentication" on that basis) — that attackers chained together to achieve unauthenticated root command execution [1][2].
- Rapid7's managed detection team observed active, targeted exploitation of internet-facing SMA 1000 appliances beginning in late June 2026, weeks before SonicWall's public advisory, and traced the chain to a websocket proxy endpoint (`/wsproxy`) pivoting into a path-traversal flaw in the appliance's hotfix-removal workflow [2].
- Compromised appliances were used as a durable beachhead rather than a one-time entry point: attackers harvested administrator credentials, session databases, and TOTP seeds, then authenticated directly to victims' internal Active Directory environments without ever reconnecting through the VPN tunnel [2].
- Within the same Rapid7 telemetry, a threat actor affiliated with the Inc ransomware-as-a-service operation was separately observed exploiting the same pair of flaws as zero-days against healthcare, financial services, and government networks, a pattern consistent with how quickly criminal groups have operationalized edge-device vulnerabilities in recent years [2][7].
- CISA added both CVEs to its Known Exploited Vulnerabilities catalog on July 14, 2026, triggering a July 17, 2026 remediation deadline for federal civilian agencies under Binding Operational Directive 22-01 [4][5]; SonicWall has published hotfixes and forensic guidance, and no interim workaround exists [3].
- This incident extends a multi-year pattern of ransomware-affiliated actors treating internet-facing SSL-VPN and remote-access appliances — from SonicWall's own SMA 100 line to Ivanti, Citrix NetScaler, and Fortinet products — as the preferred initial-access vector into enterprise networks [8][9][10][11][12].

Background

SMA 1000: SonicWall's Enterprise Remote-Access Gateway

The SMA 1000 series is SonicWall's enterprise-grade secure remote access product line, distinct from the smaller-business SMA 100 series that has separately drawn scrutiny in prior years. SMA 1000 appliances — sold as the SMA 6210, 7210, and 8200v hardware and virtual models, along with the associated Central Management Server (CMS) — sit at the network edge and broker authenticated access from remote users into internal applications, effectively functioning as a modern SSL-VPN concentrator with a web-based portal called WorkPlace and a separate administrative interface called the Appliance Management Console (AMC). Because these appliances are deliberately exposed to the internet so that remote employees can reach them, and because they are granted broad internal network reachability once a session is established, they occupy the same high-value position in an attacker's kill chain as a domain controller or an identity provider: compromise one appliance, and an attacker inherits a trusted vantage point inside the perimeter it was built to protect.

SonicWall disclosed CVE-2026-15409 and CVE-2026-15410 on July 14, 2026, crediting its own Product Security Incident Response Team analyst Adam Babis with the initial discovery, alongside independent investigative work from Volexity researchers Sean Koessel and Steven Adair [1][3][6]. The advisory confirmed both vulnerabilities were being actively exploited in the wild at the time of disclosure, a status that places this incident firmly in the category of zero-day exploitation rather than a patch-before-disclosure scenario. Affected firmware spans the 12.4.3 and 12.5.0 branches up through builds 12.4.3-03434 and 12.5.0-02800 respectively; SonicWall's fix requires upgrading to 12.4.3-03453 or 12.5.0-02835 or later via the mysonicwall.com portal [3].

A Familiar Product Line, A New Attack Surface

SonicWall's remote-access product family has a documented history of serving as an attacker entry point. CVE-2021-20016, a SQL injection flaw in the SMA 100 series, was exploited by DarkSide-affiliated ransomware operators in 2021 [8], and a succession of SMA 100 vulnerabilities were exploited in subsequent years: CVE-2023-44221 and CVE-2024-38475 were chained by attackers to steal administrator session tokens and execute commands on the appliance [9], SonicWall's SSL-VPN infrastructure was targeted in a 2025 Akira ransomware campaign built on stolen and reused credentials tied to CVE-2024-40766 [10], and a separate threat cluster tracked as UNC6148 deployed the "Overstep" backdoor against fully patched SMA 100 devices beginning in mid-2025 [11]. What

distinguishes the current incident is the product line: CVE-2026-15409 and CVE-2026-15410 affect the architecturally separate SMA 1000 series, indicating that SonicWall's exposure to this class of vulnerability is not confined to a single legacy codebase but recurs across its remote-access portfolio.

This pattern is not unique to SonicWall. Over the same period, Ivanti Sentry, Citrix NetScaler, and Fortinet's FortiOS SSL-VPN component have each disclosed critical, actively exploited vulnerabilities carrying CVSS scores at or near the maximum, including Ivanti Sentry's CVE-2026-10520, a pre-authentication command injection flaw scored CVSS 10.0 that grants root-level command execution [13], and Citrix's CVE-2026-3055, a SAML-endpoint memory-overread flaw that researchers have nicknamed "CitrixBleed 3" for its resemblance to the token-theft mechanics of the 2023 CitrixBleed campaign [14]. Security researchers tracking this trend have concluded that internet-exposed SSL-VPN and remote-access gateways have become a structural liability across the industry — they are internet-facing by design, run complex proprietary request-parsing code, and hold the credentials and trust relationships needed to reach everything behind them — even as vendors point to compensating controls such as web application firewalls and virtual patching as partial mitigations [12]. The SonicWall SMA 1000 disclosure is best read as the latest instance of that pattern rather than an isolated incident.

Security Analysis

The Exploitation Chain

Rapid7's managed detection and response team, which observed and documented exploitation independently of SonicWall's disclosure, described a two-stage chain that converts unauthenticated network access into root-level code execution [2]. The first stage abuses CVE-2026-15409, an SSRF vulnerability in the websocket-proxy feature (`/wsproxy`) underlying the SMA 1000's WorkPlace portal. By supplying a crafted host parameter, an unauthenticated remote attacker can direct the appliance to proxy websocket traffic to local-only services that are not otherwise reachable from outside the device — including, in Rapid7's testing, the appliance's internal Erlang process listening on port 1050. This effectively grants the attacker a foothold on services running behind the appliance's own network boundary, without needing valid credentials.

The second stage escalates that foothold to root. CVE-2026-15410 is a path-traversal flaw in the Appliance Management Console's hotfix-removal workflow: by submitting a crafted POST request to the `rollbackConfirm.action` endpoint with directory-traversal sequences, an attacker can cause the appliance to execute a staged shell script with root privileges as part of the (spoofed) hotfix-removal process, immediately before a system reboot [2]. Chained together, the SSRF grants the access needed

to reach the vulnerable AMC workflow, and the path traversal converts that access into full administrative control of the underlying operating system — a progression from anonymous network visitor to root operator with no authentication step in between.

Post-Exploitation Behavior and the Appliance-as-Backdoor Pattern

What makes this incident notable from a defensive standpoint is not only the technical chain but what attackers did with the access it granted. Rapid7 documented systematic harvesting of high-value material from compromised appliances: administrator credentials, session databases, and time-based one-time password (TOTP) seeds used for multi-factor authentication [2]. Armed with harvested TOTP seeds, attackers were then observed authenticating directly to victims' internal Active Directory infrastructure — bypassing the VPN tunnel entirely, since the stolen credentials and MFA material worked just as well through any other exposed authentication surface. This behavior confirms that the compromised SMA appliance functioned less as a single point of failure and more as a durable intelligence-gathering platform: once an attacker controls the device that brokers remote identity into the network, multi-factor authentication tied to seeds issued or stored on the appliance ceases to provide meaningful protection, because the appliance itself was the source of truth the attacker subverted.

Rapid7 published a set of forensic indicators that organizations can use to assess prior compromise even after patching. These include `extraweb_access.log` entries referencing the `/wsproxy` endpoint with anomalous port parameters (observed as `=-3389` in Rapid7's telemetry), `ctrl-service.log` entries showing the `remove_hotfix` function invoked with path-traversal sequences rather than a legitimate hotfix identifier, and authentication events originating from the appliance's internal management IP address under non-corporate workstation naming conventions, including hostnames resembling penetration-testing tools such as "KALI" [2]. SonicWall's own advisory echoes this guidance, directing administrators to review logs for anomalous requests to internal API endpoints before concluding an appliance is clean [3].

Independent Exploitation by Ransomware Operators

Within the same Rapid7 telemetry, a threat actor affiliated with the Inc ransomware-as-a-service operation was separately observed exploiting the same CVE-2026-15409/CVE-2026-15410 pair as zero-days against enterprise networks in healthcare, financial services, and government sectors [2][7]. The Inc-linked actor followed a similar playbook — using the SSRF-to-code-injection chain for initial access, then harvesting credentials and session data to move laterally toward domain controllers — which suggests the exploit chain was independently discovered, reverse-engineered from early attacker traffic,

or shared within criminal circles well before broad public disclosure. The presence of both an apparent espionage-oriented intrusion set and a distinct ransomware affiliate exploiting the same zero-day chain, both surfaced through Rapid7's own telemetry, is consistent with the pattern seen in prior edge-appliance incidents, where a narrow window between first exploitation and public disclosure is aggressively exploited by multiple, unrelated threat actors racing to establish footholds before patches close the opportunity.

Recommendations

Immediate Actions

Organizations operating SMA 1000 series appliances — the 6210, 7210, and 8200v hardware or virtual models, or an associated CMS instance — should upgrade to firmware 12.4.3-03453, 12.5.0-02835, or later immediately via mysonicwall.com; SonicWall has confirmed no interim workaround exists for either vulnerability, so patching is the only remediation path [3]. Before or immediately after patching, administrators should review `extraweb_access.log` and `ctrl-service.log` for the indicators Rapid7 published — anomalous `/wsproxy` requests and `remove_hotfix` invocations containing path-traversal sequences — to determine whether the appliance shows signs of prior compromise rather than assuming a clean patch history [2][3]. Any appliance exhibiting these indicators should be treated as fully compromised: SonicWall's guidance calls for re-imaging hardware appliances or redeploying virtual instances from a known-good image, rather than attempting to remediate in place, given the root-level access the attack chain provides [3].

Short-Term Mitigations

Because compromised appliances were used to harvest and replay credentials and TOTP seeds directly against Active Directory, patching the appliance alone does not remediate an organization that shows compromise indicators. Affected organizations should reset all administrator and user passwords associated with the SMA deployment and invalidate and reissue TOTP seeds for every account with access through the appliance, since a stolen seed remains valid for authentication anywhere it is accepted, independent of the VPN's own health [2][3]. Security teams should also audit recent Active Directory authentication logs for sign-ins that used SMA-associated identities but originated from IP ranges or device fingerprints inconsistent with the appliance's own network position, since this was the

specific lateral-movement technique Rapid7 documented. Organizations that cannot immediately confirm a clean forensic state should treat every credential that has ever transited the appliance as potentially exposed until proven otherwise.

Strategic Considerations

The recurrence of critical, actively exploited vulnerabilities across SonicWall's own product lines, and across the wider category of internet-facing SSL-VPN and remote-access gateways from Ivanti, Citrix, and Fortinet, suggests that patch-and-monitor operational practices are no longer sufficient on their own for this class of device [12][13][14]. Organizations with significant dependence on perimeter VPN concentrators for remote access should treat this incident as a forcing function to evaluate architectural alternatives that do not concentrate broad internal network trust in a single internet-facing appliance, such as identity-centric, application-layer access models built around the software-defined perimeter (SDP) approach. Where legacy VPN concentrators must remain in place during a transition period, organizations should prioritize reducing the appliance's implicit network reach — for example, by restricting the internal destinations a WorkPlace or equivalent session can reach to only the specific applications a given user requires — so that a future appliance compromise yields a narrower blast radius than the one observed in this incident.

CSA Resource Alignment

This incident illustrates the architectural problem CSA's Zero Trust research program was built to address: the breadth of the resulting compromise was magnified by the fact that the SMA 1000 appliance was designed and deployed as a broad network-layer gateway rather than an identity- and application-scoped access point — an architectural choice that turned two chained software defects into unrestricted internal network reach. CSA's Software-Defined Perimeter: Architecture Guide V3 provides vendor-neutral guidance for replacing exactly this kind of perimeter concentrator with an identity-first, "authenticate-before-connect" overlay model, in which a compromised access component provides significantly narrower lateral reach, because no implicit network trust is extended beyond the specific application a session was authorized for [15]. Organizations reassessing their SMA 1000 or equivalent VPN architecture in the wake of this disclosure should treat the SDP guide's transaction-flow mapping and policy-enforcement model as the target architecture, not merely a future-state ambition.

CSA's Defining the Zero Trust Protect Surface guidance is similarly applicable to the remediation decisions organizations face today. The document's core discipline — explicitly identifying the data, applications, assets, and services that a given access point is meant to reach, and constraining

connectivity to that defined protect surface — is the control that appears to have been absent in this incident, where a single compromised appliance provided attackers a path to domain controllers and broader internal infrastructure [16]. Applying this discipline to any remaining SSL-VPN or remote-access appliance, whether from SonicWall or another vendor, would materially reduce the post-compromise blast radius that made this SMA 1000 incident consequential beyond the initial appliance itself.

Finally, for organizations where an SMA 1000 or equivalent appliance mediates remote access into AI development or inference infrastructure — an increasingly common deployment pattern as AI workloads sit behind the same VPN concentrators used for conventional enterprise access — CSA's AI Controls Matrix (AICM) v1.1 offers a control-level framework, spanning its threat-and-vulnerability-management and identity-and-access-management domains, for the accelerated patching, forensic review, and credential-invalidation actions this incident demands [17]. Organizations in that position should document their SMA 1000 remediation — patch timing against the July 17, 2026 KEV deadline, forensic log review, and TOTP/credential reset — as evidence of conformance with those domains' vulnerability-response and credential-hygiene requirements.

References

[1] The Hacker News. "Two SonicWall SMA 1000 Zero-Days Exploited, One Could Enable Admin Commands." The Hacker News, July 2026.

[2] Rapid7. "Rapid7 MDR Team Discovers New SonicWall SMA1000 Zero Days Being Actively Exploited (CVE-2026-15409, CVE-2026-15410)." Rapid7 Blog, July 2026.

[3] SonicWall. "Product Notice: SMA 1000 Series Affected by Multiple Vulnerabilities." SonicWall Product Security Notice, July 14, 2026.

[4] Cybersecurity and Infrastructure Security Agency. "Known Exploited Vulnerabilities Catalog." CISA, accessed July 20, 2026.

[5] Cybersecurity and Infrastructure Security Agency. "BOD 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities." CISA, November 2021.

[6] Help Net Security. "SonicWall SMA Appliances Targeted in Zero-Day Attacks (CVE-2026-15409, CVE-2026-15410)." Help Net Security, July 14, 2026.

[7] Dark Reading. "Inc Ransomware Exploits SonicWall SMA Zero-Days." Dark Reading, July 2026.

[8] SecurityWeek. "SonicWall Zero-Day Exploited by Ransomware Group Before It Was Patched." SecurityWeek, February 2021.

[9] watchTowr Labs. "SonicBoom: From Stolen Tokens to Remote Shells — SonicWall SMA (CVE-2023-44221, CVE-2024-38475)." watchTowr Labs, 2025.

[10] Arctic Wolf. "Smash and Grab: Aggressive Akira Campaign Targets SonicWall VPNs, Deploys Ransomware in an Hour or Less." Arctic Wolf, 2025.

[11] Google Cloud. "Ongoing SonicWall Secure Mobile Access (SMA) Exploitation Campaign Using the OVERSTEP Backdoor." Google Cloud Blog, July 2025.

[12] Infosecurity Magazine. "New Fortinet and Ivanti Zero Days Exploited in the Wild." Infosecurity Magazine, 2026.

[13] Rapid7. "CVE-2026-10520, CVE-2026-10523 — Multiple Critical Vulnerabilities Affecting Ivanti Sentry." Rapid7 Blog, June 2026.

[14] Picus Security. "CVE-2026-3055 & CVE-2026-4368: Inside the NetScaler 'CitrixBleed 3' Memory Overread." Picus Security Blog, 2026.

[15] Cloud Security Alliance. "Software-Defined Perimeter: Architecture Guide V3." CSA Zero Trust Working Group, 2025.

[16] Cloud Security Alliance. "Defining the Zero Trust Protect Surface." CSA Zero Trust Working Group, 2024.

[17] Cloud Security Alliance. "AI Controls Matrix (AICM) v1.1." CSA, 2026.