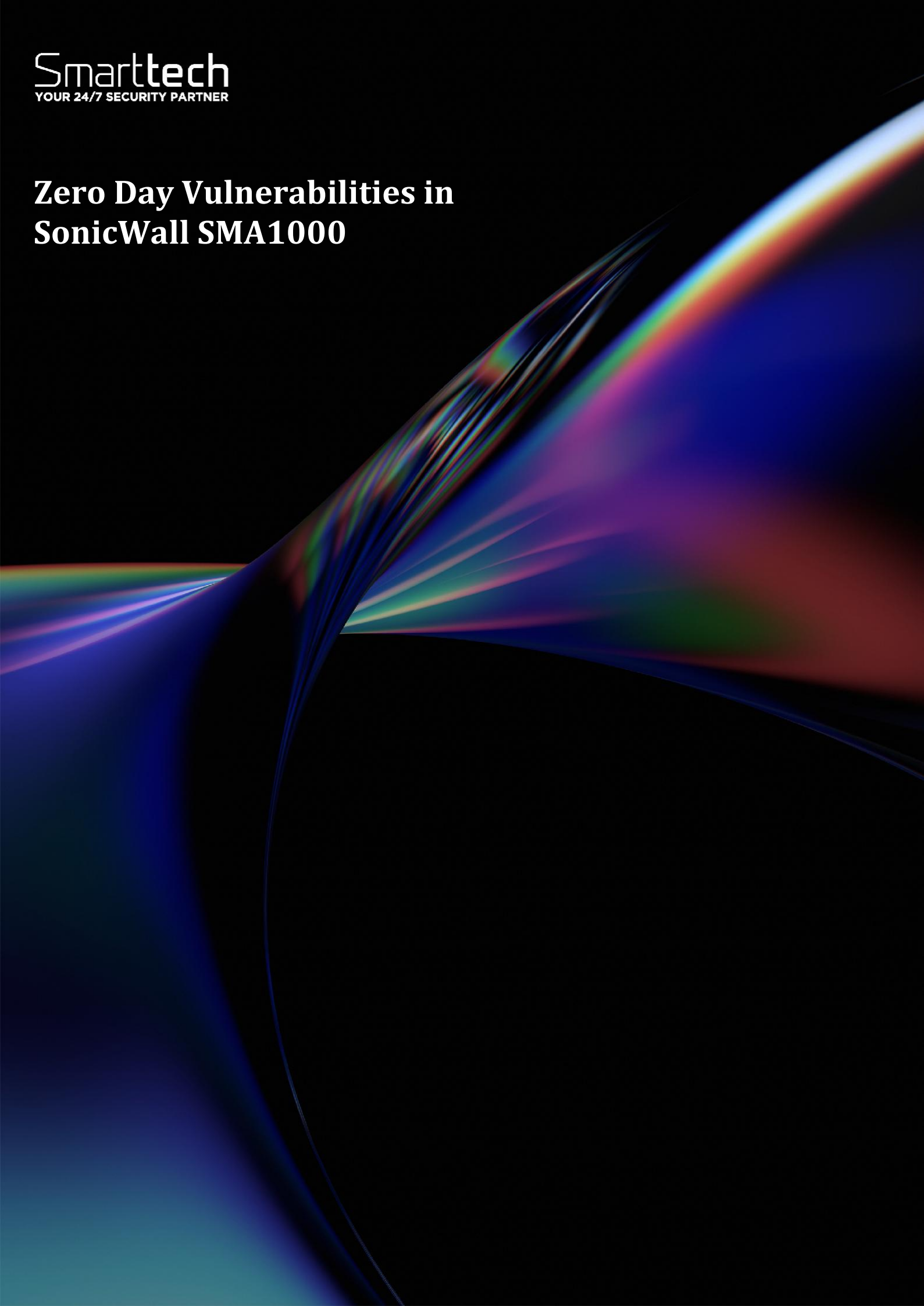
Smarttech
YOUR 24/7 SECURITY PARTNER

Zero Day Vulnerabilities in SonicWall SMA1000



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	117
Authors	Dorin Constantin Banu < constantin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-07-15
Issue Date	2026-07-14

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released. Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview:

New vulnerabilities have been identified in the SonicWall SMA 1000 appliances that are currently being exploited in the wild. Successful exploitation could allow a remote unauthenticated attacker to force the appliance to make requests to unintended locations through SSRF, and under specific conditions enable a remote authenticated administrator to execute arbitrary operating system commands via code injection.

Risk:

Government:

- Large and medium government entities: Critical
- Small government entities: High

Businesses:

- Large and medium business entities: Critical
- Small business entities: High

Technical summary:

CVE	*Description*
CVE-2026-15409 **CVSS Score: 10** **A Server-side request forgery (SSRF)**	A Server-side request forgery (SSRF) vulnerability has been identified in the SMA1000 Appliance Work Place interface. A remote unauthenticated attacker could potentially cause the appliance to make requests to unintended location.
CVE-2026-15410 **CVSS Score: 7.2** **Post-authentication improper control of generation of code ('Code Injection')**	Post-authentication improper control of generation of code ('Code Injection') vulnerability has been identified in the SMA1000 Appliance Management Console (AMC) which in specific conditions could potentially enable a remote authenticated attacker as administrator to execute arbitrary OS commands.

Affected Products:

Product	*Version*
SMA1000 Models - 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)

Note: These vulnerabilities do not affect SSL-VPN running on SonicWall firewalls or the SMA 100 Series product line.

Fixed Software:

Product	*Version*
SMA1000 Models - 6210, 7210, 8200v	12.4.3-03453 (platform-hotfix) and higher versions.
	12.5.0-02835 (platform-hotfix) and higher versions.

Indicators of Compromise (IOCs):

Customers should review logs for signs including, but not limited to:

- if in extraweb_access.log are mentioned requests to /__api__/login or /__api__/logout with http 200 status
- if in extraweb_access.log are mentioned requests to /wsproxy with suspicious host parameters with 101 http status
- if in ctrl-service.log are mentioned hotfix rollbacks with path traversal names
- if /var/lib/unit/conf.json contains routes for /__api__/login or /__api__/logout (these URIs do not exist in legitimate configuration)

If IOCs are present on the system, customers should:

- re-image (hardware) or re-deploy (virtual) appliances.
- change user & administrator passwords.
- reset TOTP tokens

Recommendations

We recommend the following actions be taken:

- Apply appropriate updates, hot fixes or mitigations provided by SonicWall to vulnerable systems immediately after appropriate testing. (**M1051: Update Software**)
    - **Safeguard 7.1 : Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 7.2: Establish and Maintain a Remediation Process:** Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
    - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
    - **Safeguard 7.5: Perform Automated Vulnerability Scans of Internal Enterprise Assets:** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.

    - **Safeguard 7.7: Remediate Detected Vulnerabilities:** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
    - **Safeguard 12.1: Ensure Network Infrastructure is Up-to-Date:** Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.
    - **Safeguard 18.1: Establish and Maintain a Penetration Testing Program:** Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.
    - **Safeguard 18.2: Perform Periodic External Penetration Tests:** Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.
    - **Safeguard 18.3: Remediate Penetration Test Findings:** Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.
- Use network appliances to filter ingress or egress traffic and perform protocol-based filtering. Configure software on endpoints to filter network traffic. **(M1037: Filter Network Traffic)**
    - **Safeguard 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure:** Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 7.6: Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets:** Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.
    - **Safeguard 7.7: Remediate Detected Vulnerabilities:** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. **(M1050: Exploit Protection)**
    - **Safeguard 10.5: Enable Anti-Exploitation Features:** Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.

References

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

CVEs

CVE-2026-15409
CVE-2026-15410

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com