مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Actively Exploited Vulnerabilities in SonicWall SMA1000

Tracking #:432319297

Date:15-07-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed SonicWall has released a critical security advisory addressing two actively exploited vulnerabilities affecting SMA1000 Series Secure Mobile Access appliances.

TECHNICAL DETAILS:

SonicWall has released a critical security advisory addressing two vulnerabilities affecting SMA1000 Series Secure Mobile Access appliances. The vulnerabilities, tracked as CVE-2026-15409 and CVE-2026-15410, include a critical unauthenticated Server-Side Request Forgery (SSRF) vulnerability and a high-severity post-authentication Code Injection vulnerability.

According to SonicWall Product Security Incident Response Team (PSIRT), both vulnerabilities are being actively exploited in the wild. Organizations using affected SMA1000 appliances should immediately apply the latest platform hotfixes and perform compromise assessments to identify any unauthorized activity.

The SSRF vulnerability carries the maximum CVSS v3 score of 10.0, enabling remote unauthenticated Organizations should prioritize deployment of these updates, particularly for Active Directory Federation Services (AD FS) and Microsoft SharePoint Server, as both have already been exploited by threat actors.

Exploited Vulnerability Details:

1. **CVE-2026-15409 – Server-Side Request Forgery (SSRF)**
   - CVSS: 10.0 (Critical)
   - CWE: CWE-918 – Server-Side Request Forgery (SSRF)
   - Attack Vector: Network
   - Authentication Required: None
   - User Interaction: None
   - A critical Server-Side Request Forgery (SSRF) vulnerability exists in the SMA1000 Appliance Work Place interface.
   - A remote, unauthenticated attacker can force the appliance to send requests to unintended internal or external destinations.
   - Successful exploitation may allow attackers to access internal services, bypass network restrictions, and facilitate further compromise.
2. **CVE-2026-15410 – Code Injection**
   - CVSS: 7.2 (High)
   - CWE: CWE-94 – Improper Control of Generation of Code ('Code Injection')
   - Attack Vector: Network
   - Authentication Required: Administrator privileges
   - User Interaction: None
   - Vulnerability Details
   - A post-authentication Code Injection vulnerability exists in the SMA1000 Appliance Management Console (AMC).
   - Under specific conditions, an authenticated administrator can execute arbitrary operating system commands.
   - Successful exploitation could result in complete system compromise.

- The vulnerability impacts the appliance management interface.

Affected Products:

Affected Appliances

- SonicWall SMA1000 Series
  - SMA 6210
  - SMA 7210
  - SMA 8200v

Affected Versions

12.4.x

- 12.4.3-03245
- 12.4.3-03387
- 12.4.3-03434 (platform-hotfix)

12.5.x

- 12.5.0-02283
- 12.5.0-02624
- 12.5.0-02800 (platform-hotfix)

Not Affected

- SonicWall Firewall SSL-VPN
- SonicWall SMA 100 Series appliances

Fixed Versions

- 12.4.3-03453 (platform-hotfix) or later
- 12.5.0-02835 (platform-hotfix) or later

Indicators of Compromise (IoCs)

Administrators 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)

RECOMMENDATIONS:

Immediate Actions:

- Upgrade affected appliances to fixed version or later platform-hotfix releases.
- Conduct a comprehensive forensic investigation to determine whether unauthorized access has occurred.
- If compromise is detected:
  - Re-image physical appliances or re-deploy virtual appliances.
  - Change all user and administrator passwords.
  - Reset all TOTP/MFA tokens.
  - Rotate service account credentials and API keys stored on the appliance.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

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