CYBER ADVISORY

Thursday, December 18, 2025 **CAL-CSIC-202512-A-012**

SonicWall SMA 1000 Privilege Escalation Vulnerability

Chained Vulnerability	Privilege Escalation	Active Exploitation	Patch Available

The California Cybersecurity Integration Center (Cal-CSIC) has identified a local privilege escalation vulnerability in the appliance management console (AMC) of the SonicWall SMA 1000 appliance. CVE-2025-2025-40602 carries a CVSS 3.1 score of 6.6.[1] Successful exploitation allows an authenticated, remote attacker to escalate privileges on an affected device. SonicWall has stated that CVE 2025-40602 has been exploited in a chained attack with CVE-2025-23006 (CVSS 9.8), a deserialization of untrusted data vulnerability that was patched in January 2025. The combination of these two vulnerabilities would allow an unauthenticated attacker to execute arbitrary code with *root* privileges. CVE-2025-40602 does not have a publicly available Proof-of-Concept and has been discovered to be exploited in the wild. The vendor has issued a security advisory with a workaround and a patch for affected appliances.[2]

Analyst Comment: *Although CVE-2025-40602 has been reported to be chained with CVE-2025-23006, it should be noted that the only known exploitation paths for CVE-2025-40602 are SonicWall SMA 1000 appliances that remain unpatched to CVE-2025-23006, or that the threat actor already possesses access to the local system.*

The Cal-CSIC recommends immediately following SonicWall's guidance and deploying the latest security patch. If immediate patching is delayed, please follow SonicWall's guidance for applying workarounds.[3]

For further information on applying SonicWall's security patch and workarounds please use this link:

Security Advisory

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0019

Affected Product:

Product	Version
SMA 1000	12.4.3-03093 (platform-hotfix) and earlier versions. 12.5.0-02002 (platform-hotfix) and earlier versions.

References

[1] NVD; CVE-2025-40602 Detail; https://nvd.nist.gov/vuln/detail/CVE-2025-40602; accessed 18 December 2025
[2] Tenable; CVE-2025-40602: SonicWall Secure Mobile Access (SMA) 1000 Zero-Day Exploited; https://www.tenable.com/blog/cve-2025-40602-sonicwall-secure-mobile-access-sma-1000-zero-day-exploited; accessed 18 December 2025
[3] SonicWall; Vulnerability List; https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0019; accessed 18 December 2025