Posting Date: 2026/09/10

Vulnerability Alert Multiple High-Risk Security Vulnerabilities Found in SonicWall NSM On-Prem and SMA1000 Series (CVE-2026-78327, CVE-2026-83548, and CVE-2026-83549), Please Confirm and Patch Promptly

- Subject: Vulnerability Alert Multiple High-Risk Security Vulnerabilities Found in SonicWall NSM On-Prem and SMA1000 Series (CVE-2026-78327, CVE-2026-83548, and CVE-2026-83549), Please Confirm and Patch Promptly

- Description:
  - Forwarding National Information Sharing and Analysis Center Cybersecurity Alert NISAC-200-202609-00000008
  - Researchers have discovered multiple high-risk security vulnerabilities (CVE-2026-78327, CVE-2026-83548, and CVE-2026-83549) in SonicWall NSM On-Prem and SMA1000 Series, including OS Command Injection and Server-Side Request Forgery (SSRF). Among them, CVE-2026-83548 and CVE-2026-83549 have already been exploited by hackers. Please confirm and perform patching as soon as possible.
  - CVE-2026-78327 An authenticated remote attacker with administrative privileges could execute arbitrary code on the underlying host by injecting arbitrary OS commands into the management interface.
  - CVE-2026-83548 An unauthenticated remote attacker could leverage an unexpected alternative access path to access sensitive functions and perform unauthorized operations.
  - CVE-2026-83549 Under specific conditions, an authenticated remote attacker could execute arbitrary OS commands as an administrator via the Appliance Management Console (AMC), thereby executing arbitrary code.
- Affected Platforms:
  - SonicWall NSM On-Prem (VMware, Hyper-V, Azure, and KVM) version 4.3.0 (inclusive) and earlier versions
  - SonicWall SMA1000 Series (6210, 7210, and 8200v) platform-hotfix version 12.4.3-03453 (inclusive) and earlier versions
  - SonicWall SMA1000 Series (6210, 7210, and 8200v) platform-hotfix version 12.5.0-02835 (inclusive) and earlier versions
- Recommended Actions:
  - Official fix updates for the vulnerabilities have been released. Please refer to the official instructions to apply updates at the following links:
    1. https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0015
    2. https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0016

- References:
  1. https://nvd.nist.gov/vuln/detail/CVE-2026-78327
  2. https://nvd.nist.gov/vuln/detail/CVE-2026-83548
  3. https://nvd.nist.gov/vuln/detail/CVE-2026-83549

Computer and Communication Center
Network System Division