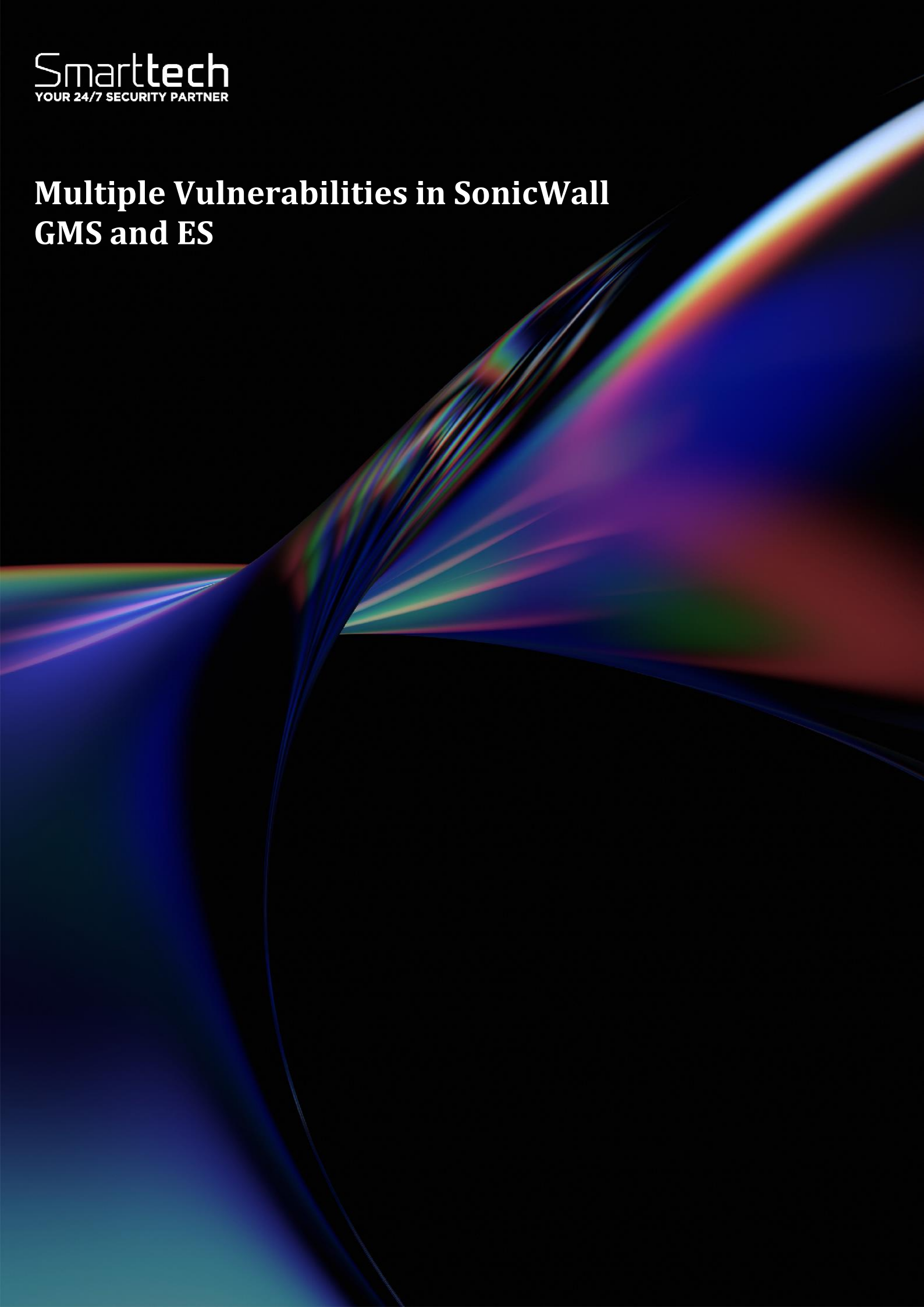
Smarttech
YOUR 24/7 SECURITY PARTNER

Multiple Vulnerabilities in SonicWall GMS and ES



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	135
Authors	Gabriel Gheorghiu <gabriel.gheorghiu@smarttech247.com>
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-08-12
Issue Date	2026-08-12

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:

Multiple vulnerabilities have been identified across SonicWall Global Management System (GMS) and SonicWall Email Security (ES) products. The disclosed flaws include critical unauthenticated remote code execution, authenticated command injection, privilege escalation, cross-site scripting (XSS), arbitrary file write, and certificate validation weaknesses. Successful exploitation could allow attackers to execute arbitrary code, obtain elevated privileges, access sensitive information, perform unauthorized system modifications, compromise administrative sessions, or gain full control of affected systems.

Risk:

Government:

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

Businesses:

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

Technical summary:

Tactic: Initial Access (TA0001)
Technique: Exploit Public-Facing Application (T1190): The unauthenticated vulnerabilities affecting SonicWall GMS could be exploited remotely through exposed management services, potentially allowing attackers to execute arbitrary code, access sensitive information, and compromise affected systems without prior authentication.

Tactic: Privilege Escalation (TA0004)
Technique: Exploitation for Privilege Escalation (T1068): Multiple vulnerabilities affecting SonicWall GMS and SonicWall Email Security could allow authenticated or low-privileged attackers to elevate privileges, execute arbitrary commands with root-level permissions, and gain unauthorized control over affected systems.

Tactic: Credential Access (TA0006)
Technique: Adversary-in-the-Middle (T1557): An insufficient certificate validation weakness in SonicWall GMS could be leveraged under successful man-in-the-middle (MitM) conditions to compromise communications and facilitate unauthorized actions

CVE	Product	Vulnerability Type	CVSS	Impact
CVE-2026-66145	SonicWall GMS	Remote Code Execution (Zip Slip)	9.1 Critical	Sensitive data exposure, arbitrary file write

CVE-2026-66147	SonicWall GMS	Command Injection / RCE	9.4 Critical	Remote code execution via crafted requests
CVE-2026-66154	SonicWall GMS	Improper Certificate Validation	8.3 High	User compromise through MitM attack
CVE-2026-18634	SonicWall GMS	Insecure Deserialization	8.4 High	Privilege escalation and unauthorized actions
CVE-2026-66148	SonicWall GMS	Command Injection / Privilege Escalation	6.3 Medium	Root command execution
CVE-2026-66146	SonicWall GMS	Cross-Site Scripting (XSS)	5.5 Medium	JavaScript execution in user browser
CVE-2026-66149	SonicWall Email Security	Command Injection	7.8 High	Root command execution via netmask parameter
CVE-2026-66150	SonicWall Email Security	Command Injection	7.8 High	Root command execution via SNMP parameter

No evidence of active exploitation in the wild has been reported by SonicWall at the time of publication.

Affected Products:

Product	***Version***
GMS - Virtual Appliance and Windows	9.5.1 and earlier versions
Email Security (ES Appliance 5000, 5050, 7000, 7050, 9000, VMware and Hyper-V)	10.0.35.8405 and earlier versions.

Workaround:

No official workaround has been provided by SonicWall for the vulnerabilities addressed in SNWLID-2026-0011 and SNWLID-2026-0012.

Fixed Software:

Product	***Version***
GMS - Virtual Appliance and Windows	9.5.2
Email Security (ES Appliance 5000, 5050, 7000, 7050, 9000, VMWare and Hyper-V)	10.0.36 and higher versions.

Recommendations

We recommend the following actions be taken:

- Apply appropriate updates 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.
- 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 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.

References

https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0012
https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0011

CVE

CVE-2026-66149
CVE-2026-66150
CVE-2026-66145
CVE-2026-66146
CVE-2026-66147
CVE-2026-66148
CVE-2026-66154
CVE-2026-18634


Smarttech
YOUR 24/7 SECURITY PARTNER
www.smarttech247.com