

# CVE-2026-15410

## SonicWall SMA1000 Appliances Code Injection Vulnerability

CISA KEV since Jul 14, 2026

Actively exploited

Ransomware use known

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.

|                                                                |                                                      |                                                                  |                                                                                                    |
|----------------------------------------------------------------|------------------------------------------------------|------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| <p>EVRS</p> <p><b>75</b>/100</p> <p><b>Urgent</b> priority</p> | <p>CVSS V3.1</p> <p><b>7.2</b></p> <p>High · NVD</p> | <p>EPSS</p> <p><b>0.118</b></p> <p>96.1st percentile · FIRST</p> | <p>CISA DEADLINE</p> <p><b>Jul 17, 2026</b></p> <p>CISA federal deadline · Overdue by 3 months</p> |
|----------------------------------------------------------------|------------------------------------------------------|------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|

### Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

|                                                       |                            |                                                                |                                        |
|-------------------------------------------------------|----------------------------|----------------------------------------------------------------|----------------------------------------|
| <input checked="" type="checkbox"/> <b>CISA KEV</b>   | Listed in the catalog      | <input type="checkbox"/> <b>Vendor exploitation</b>            | Confirmed exploitation in the wild     |
| <input checked="" type="checkbox"/> <b>Ransomware</b> | Known ransomware campaigns | <input type="checkbox"/> <b>KEV recency</b>                    | Added to CISA KEV within the last year |
| <input checked="" type="checkbox"/> <b>EPSS</b>       | 0.118 probability          | <input type="checkbox"/> <b>Pre-patch disclosure</b>           | Disclosure status unavailable          |
| <input checked="" type="checkbox"/> <b>CVSS</b>       | Base score 7.2             | <input type="checkbox"/> <b>Microsoft Exploitability Index</b> | Not a Microsoft CVE                    |

### Remediation

**Patch This Cycle** Patch or fixed version identified

**CISA required action:** Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines.  
Basis: CISA KEV required action

### Affected and fixed versions

| PACKAGE          | AFFECTED                                                                                     | FIXED IN                | SOURCE |
|------------------|----------------------------------------------------------------------------------------------|-------------------------|--------|
| sma8200v         | 12.4.3-03245<br>12.4.3-03387<br>12.4.3-03434<br>12.5.0-02283<br>12.5.0-02624<br>12.5.0-02800 | no fixed version listed | NVD    |
| sma6210 firmware | 12.4.3-03245<br>12.4.3-03387<br>12.4.3-03434<br>12.5.0-02283<br>12.5.0-02624<br>12.5.0-02800 | no fixed version listed | NVD    |
| sma7210 firmware | 12.4.3-03245<br>12.4.3-03387<br>12.4.3-03434<br>12.5.0-02283<br>12.5.0-02624<br>12.5.0-02800 | no fixed version listed | NVD    |

| PACKAGE | AFFECTED | FIXED IN                | SOURCE |
|---------|----------|-------------------------|--------|
| sma6210 | –        | no fixed version listed | NVD    |
| sma7210 | –        | no fixed version listed | NVD    |

## Sources

|                        |                                                                                                                                                                                             |                                      |                                                                                                                                                                                                                                             |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Vendor guidance</b> | <a href="https://github.com/advisories/GHSA-pxc4-295p-35qq">github.com/advisories/GHSA-pxc4-295p-35qq</a>                                                                                   | <b>Additional guidance</b>           | <a href="https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0008">psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0008</a>                                                                                                       |
| <b>BOD 26-04</b>       | <a href="https://cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk">cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk</a> | <b>Forensics Triage Requirements</b> | <a href="https://cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk">cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk</a> |
| <b>NVD</b>             | <a href="https://nvd.nist.gov/vuln/detail/CVE-2026-15410">nvd.nist.gov/vuln/detail/CVE-2026-15410</a>                                                                                       | <b>CISA KEV</b>                      | <a href="https://cisa.gov/known-exploited-vulnerabilities-catalog">cisa.gov/known-exploited-vulnerabilities-catalog</a>                                                                                                                     |
| <b>ENISA EUVD</b>      | <a href="https://euvd.enisa.europa.eu/vulnerability/EUVD-2026-44410">euvd.enisa.europa.eu/vulnerability/EUVD-2026-44410</a>                                                                 | <b>Current data</b>                  | <a href="https://evulnable.com/vulnerability-management/cve/CVE-2026-15410">evulnable.com/vulnerability-management/cve/CVE-2026-15410</a>                                                                                                   |

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.