CERT-EU

Security Advisory 2022-022

Critical RCE Vulnerability in SonicWall Firewalls

March 29, 2022 — v1.0

TLP:WHITE

History:

- *29/03/2022 — v1.0 – Initial publication*

Summary

On 25/03/2022, SonicWall has fixed a critical vulnerability (CVE-2022-22274) [2] in SonicWall firewall product, which allows remote unauthenticated attacker to cause Denial-of-Service (DoS) that potentially results in code execution in the firewall. This vulnerability has a score of 9.4 out of 10 [1].

CERT-EU strongly recommends to patch this vulnerability **as soon as possible**.

Technical Details

A stack-based buffer overflow vulnerability in the SonicOS via HTTP request allows a remote unauthenticated attacker to cause Denial of Service (DoS) that potentially results in code execution in the firewall. A low complexity attack that does not require user interaction.

This vulnerability only impacts the *web management* interface, the SonicOS SSLVPN interface is not impacted.

SonicWall PSIRT is not aware of active exploitation in the wild. No reports of a PoC have been made public and malicious use of this vulnerability has not been reported to SonicWall [1].

Affected Products

Below are the list of SonicWall appliances impacted :

Impacted platforms	Impacted version	Fixed Version
TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W, TZ570P, TZ670, NSa 2700, NSa 3700, NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, NSsp 13700, NSv 270, NSv 470, NSv 870	7.0.1-5050 and older	7.0.1-5051 and higher
NSsp 15700	7.0.1-R579 and older	7.0.1-R579 and older
NSv 10, NSv 25, NSv 50, NSv 100, NSv 200, NSv 300, NSv 400, NSv 800, NSv 1600	6.5.4.4-44v-21-1452 and earlier	6.5.4.4-44v-21-1519 and higher

The following firewall platforms are not impacted :

Firewall Generations	Platforms Not Impacted
Gen5	SOHO, TZ100, TZ100W, TZ105, TZ105W, TZ200,TZ200W, TZ205, TZ205W, TZ210, TZ210W, TZ215, TZ215W, NSA220, NSA220W, NSA240, NSA2400, NSA2400MX, NSA250M, NSA250MW, NSA3500, NSA4500, NSA5000 NSAE5500, NSAE6500, NSAE7500, NSAE8500, NSAE8510
Gen6	SOHOW, SOHO 250, SOHO 250W, TZ300, TZ300P, TZ300W, TZ350, TZ350W, TZ400, TZ400W, TZ500, TZ500W, TZ600, TZ600P, NSA 2600, NSA3600, NSA4600, NSA5600, NSA6600, SM9200, SM9400, SM9600, SM9800, SM10200, SM10400, SM10800, NSsp12400, NSsp12800
Gen 6.5	NSa 2650, NSa3650, NSa4650, NSa5650, NSa6650, NSa9250, NSa9450, NSa9650

Recommendations and Workarounds

The company has released patches for almost all impacted SonicOS versions and firewalls and urged customers to update all affected products [3].

The only affected firewall still waiting for a patch against CVE-2022-22274 is the NSsp 15700 enterprise-class high-speed firewall. While a hotfix is already available for those reaching out to the support team, SonicWall estimates that a full patch to block potential attacks targeting this firewall will be released in roughly two weeks [3].

As a general workaround, it is recommended to protect from external attackers by ensuring that the SonicOS management interface is not exposed to the Internet by modifying the existing SonicOS Management access rules.

References

[1] https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003

[2] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22274

[3] https://www.bleepingcomputer.com/news/security/critical-sonicwall-firewall-patch-not-released-for-all-devices/