Security Advisory 2021-066

SonicWall Critical Vulnerabilities

December 10, 2021 — v1.0

TLP:WHITE

History:

- *10/12/2021 — v1.0 – Initial publication*

Summary

On December 7th, SonicWall released security patches to address several security vulnerabilities [1]. This list includes a critical unauthenticated stack-based buffer overflow vulnerability (CVE-2021-20038) with a CVSS score of 9.8 out of 10. If exploited, it could allow a remote unauthenticated attacker to execute code as a `nobody` user in the appliance.

There is another group of vulnerabilities, collectively tracked as CVE-2021-20045, which has a combined critical CVSS score of 9.4 out of 10. They could allow a remote unauthenticated attacker to cause heap-based and stack-based buffer overflow that would result in code execution as the `nobody` user [2].

According to SonicWall, there is no evidence that this vulnerability is being exploited in the wild.

Technical Details

CVE-2021-20038

This vulnerability is due to the SonicWall SMA SSLVPN Apache HTTPD server GET method of `mod_cgi` module environment variables use a single stack-based buffer using `strcat` [1].

CVE-2021-20045

This vulnerability is due to the `sonicfiles` `RAC_COPY_TO` (`RacNumber 36`) method which allows users to upload files to an SMB share and can be called without any authentication. `RacNumber 36` of the `sonicfiles` API maps to the `upload_file` Python method and this is associated with `filexplorer` binary. This is a custom program written in C++ which is vulnerable to a number of memory safety issues.

Affected Products

This vulnerability affects SMA100 series:

- SMA 200, 210, 400, 410 and 500v products versions `9.0.0.11-31sv*` and earlier, `10.2.0.8-37sv`, `10.2.1.1-19sv`, `10.2.1.2-24sv` and earlier.
- SMA 100 series appliances with WAF enabled are also impacted by the majority of these vulnerabilities.

Recommendations

Support for `9.0.0` firmware ended on 10/31/2021. Customers still using that firmware are requested to upgrade to the latest `10.2.x` versions.

CERT-EU strongly recommends to upgrade your affected appliance(s) to the fixed versions of the firmware (SMA `10.2.0.9-41sv`, `10.2.1.3-27sv`).

References

[1] https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0026

[2] https://threatpost.com/critical-sonicwall-vpn-bugs-appliance-takeover/176869/