Security Advisory 2022-054

Critical SQL Injection Vulnerability

July 25, 2022 — v1.0

TLP:WHITE

History:

- *25/07/2022 — v1.0 – Initial publication*

Summary

On July 21st, 2022, SonicWall released security patches for their **Analytics On-Prem** and **GMS** products, addressing a critical SQL injection flaw [1,2]. Currently, no reports of a proof of concept (PoC) have been made public and there is no active exploitation in the wild.

Nevertheless, immediate update to the patched versions is recommended.

Technical Details

The vulnerability is being tracked as CVE-2022-22280, it has been rated as critical (CVSS 9.4) and it allows **unauthenticated SQL injection** due to an Improper Neutralization of Special Elements used in an SQL command, impacting SonicWall GMS and Analytics On-Prem [1,2].

Affected Products

The following product versions are affected from this flaw:

- GMS 9.3.1-SP2-Hotfix-1 and earlier
- Analytics 2.5.0.3-2520 and earlier

Recommendations

It is strongly recommended to update to the respective fixed versions:

- GMS 9.3.1-SP2-Hotfix-2
- Analytics 2.5.0.3-Hotfix-1

Additionally, SonicWall suggests that the likelihood of exploitation may be significantly reduced by incorporating a Web Application Firewall (WAF) to block SQL injection attempts.

References

[1] https://www.sonicwall.com/support/knowledge-base/security-notice-sonicwall-gms-sql-injection-vulnerability/220613083124303/

[2] https://www.sonicwall.com/support/notices/security-notice-sonicwall-analytics-on-prem-sql-injection-vulnerability/220613083254037/