Security Advisory 2023-048

Critical Vulnerabilities in SonicWall GMS and Analytics

July 13, 2023 — v1.0

TLP:CLEAR

History:

- *13/07/2023 — v1.0 – Initial publication*

Summary

On July 12, SonicWall released an Urgent Security Notice regarding a suite of vulnerabilities, among which 4 of them rated as critical, affecting SonicWall GMS and Analytics [1].

CERT-EU recommends upgrading as soon as possible to the latest version.

Technical Details

CVE-2023-34124: This vulnerability with a CVSS score of 9.4 out of 10 could allow an unauthenticated remote attacker to bypass web services authentication mechanisms.

CVE-2023-34133: This vulnerability with a CVSS score of 9.8 out of 10 could allow an unauthenticated remote attack to inject SQL commands, and bypass security filters due to an improper neutralisation of special elements used in an SQL command.

CVE-2023-34134: This vulnerability with a CVSS score of 9.8 out of 10 could allow a remote attacker to read password hash via web services.

CVE-2023-34137: This vulnerability with a CVSS score of 9.4 out of 10 could allow an unauthenticated remote attacker to bypass CAS authentication mechanisms.

CVE-2023-34123: This vulnerability with a CVSS score of 7.5 out of 10 could allow a remote attacker to predict password reset key due to the use of hard-coded cryptographic keys.

CVE-2023-34126: This vulnerability with a CVSS score of 7.1 out of 10 could allow an authenticated remote attacker to upload arbitrary files due to insufficient checks.

CVE-2023-34127: This vulnerability with a CVSS score of 8.8 out of 10 could allow an authenticated remote attacker to execute arbitrary commands due to improper neutralisation of special elements used in an OS command.

CVE-2023-34129: This vulnerability with a CVSS score of 7.1 out of 10 could allow an authenticated remote attacker to write arbitrary files via web services due to improper limitations of a pathname to a restricted directory.

Affected Products

- GMS 9.3.2-SP1 and before
- Analytics 2.5.0.4-R7 and before

Recommendations

CERT-EU strongly recommends upgrading to the latest versions of SonicWall GMS (`v9.3.3`) and Analytics (`2.5.2`)

References

[1] https://www.sonicwall.com/support/knowledge-base/urgent-security-notice-sonicwall-gms-analytics-impacted-by-suite-of-vulnerabilities/230710150218060/