April 30, 2024

Overall Rating - High

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that SonicWall published a security advisory to address vulnerabilities in the following product:

- SonicWall GMS (Virtual Appliance, Windows) – version 9.3.4 and prior

Technical Details

onicWall GMS (Virtual Appliance, Windows) - 9.3.4 and earlier versions are vulnerable to the following security issues.
1) CVE-2024-29010 - GMS ECM Policy XML External Entity Processing Information Disclosure Vulnerability.
The XML document processed in the GMS ECM endpoint is vulnerable to XML external entity (XXE) injection vulnerability leading to information disclosure.
CVSS Score: 7.1
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N
CWE-611: Improper Restriction of XML External Entity Reference

2) CVE-2024-29011 - GMS ECM Hard-Coded Credential Authentication Bypass Vulnerability.
Use of hard-coded password in the GMS ECM endpoint leading to authentication bypass vulnerability.
CVSS Score: 7.5
CVSS Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CWE-259: Use of Hard-coded Password

These vulnerabilities are rated as an overall **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2024-29010, CVE-2024-29011
- SonicWall Security Advisory – SNWLID-2024-0007
- SonicWall Security Advisories