The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

https://www.cisa.gov/tlp

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:

12/08/2021

01/25/2022 - UPDATED

SUBJECT:

Multiple Vulnerabilities in SonicWall SMA 100 Series Could Allow for Arbitrary Code Execution

OVERVIEW:

Multiple vulnerabilities in SonicWall SMA 100 Series could allow for arbitrary code execution. Successful exploitation of these vulnerabilities could allow for arbitrary code execution. The SonicWall SMA 100 Series is a unified secure access gateway that enables organizations to provide access to any application, anytime, from anywhere and any devices, including managed and unmanaged. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Applications that are configured to have fewer user rights on the system could be less impacted than those that operate with administrative user rights.

THREAT INTELLIGENCE:

There are currently no reports of these vulnerabilities being exploited in the wild.

January 25 – UPDATED THREAT INTELLIGENCE:

NCC Group has reported that threat actors are now attempting to exploit CVE-2021-20038 in the wild, as well as attempting to brute force access via password spraying known default credentials. At the moment, there have been no confirmed successful exploitations per NCC and SonicWall PSIRT.

SYSTEMS AFFECTED:

- SonicWall SMA 100 Series 10.2.1.0-17sv and earlier
- SonicWall SMA 100 Series 10.2.1.1-19sv and earlier
- SonicWall SMA 100 Series 10.2.1.2-24sv and earlier
- SonicWall SMA 100 Series 9.0.0.11-31sv and earlier
- SonicWall SMA 100 Series 10.2.0.8-37sv and earlier

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities in SonicWall SMA 100 Series could allow for arbitrary code execution. Details of these vulnerabilities are as follows:

- A Unauthenticated Stack-based Buffer Overflow which could allow for an attacker to potentially execute code as a 'nobody' user in the appliance. (CVE-2021-20038)
- A Authenticated Command Injection Vulnerability as Root which could allow for an attacker to potentially execute code as a 'nobody' user in the appliance. (CVE-2021-20039)
- A Unauthenticated File Upload Path Traversal Vulnerability which could allow a remote unauthenticated attacker to upload crafted web pages or files as a 'nobody' user. (CVE-2021-20040)
- A Unauthenticated CPU Exhaustion Vulnerability which could result in DoS. (CVE-2021-20041)
- A Unauthenticated "Confused Deputy" Vulnerability which could allow an unauthenticated attacker to bypass firewall rules. (CVE-2021-20042)
- A getBookmarks Heap-based Buffer Overflow which could allow for an attacker to potentially execute code as a 'nobody' user in the appliance. (CVE-2021-20043)
- A Post-Authentication Remote Code Execution (RCE) which could allow a remote authenticated attacker to execute OS system commands in the appliance. (CVE-2021-20044)
- Multiple Unauthenticated File Explorer Heap-based and Stack-based Buffer Overflows which could allow for an attacker to potentially execute code as a 'nobody' user in the appliance. (CVE-2021-20045)

Successful exploitation of these vulnerabilities could allow for arbitrary code execution. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Applications that are configured to have fewer user rights on the system could be less impacted than those that operate with administrative user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by SonicWall to vulnerable systems immediately after appropriate testing.
- Block external access at the network boundary, unless external parties require service.
- If global access isn't needed, filter access to the affected computer at the network boundary. Restricting access to only trusted computers and networks might greatly reduce the likelihood of successful exploits.
- Run all software as a nonprivileged user with minimal access rights. To mitigate the impact of a successful exploit, run the affected application as a user with minimal access rights.
- Deploy network intrusion detection systems to monitor network traffic for malicious activity.

- Deploy NIDS to detect and block attacks and anomalous activity such as requests containing suspicious URI sequences. Since the webserver may log such requests, review its logs regularly.
- Implement multiple redundant layers of security. Since this issue may be leveraged to execute code, we recommend memory-protection schemes, such as nonexecutable stack/heap configurations and randomly mapped memory segments. This tactic may complicate exploit attempts of memory-corruption vulnerabilities.

REFERENCES:
CVE(s):
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20038
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20039
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20040
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20041
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20042
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20043
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20044
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20045

SonicWall:
https://www.sonicwall.com/support/product-notification/product-security-notice-sma-100-series-vulnerability-patches-q4-2021/211201154715443/

January 25 – UPDATED REFERENCES:
BleepingComputer:
https://www.bleepingcomputer.com/news/security/attackers-now-actively-targeting-critical-sonicwall-rce-bug/