*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:**

09/27/2021

**SUBJECT:**

A Vulnerability in SonicWall SMA 100 Series Could Allow for Arbitrary File Deletion

**OVERVIEW:**

A vulnerability has been discovered in SonicWall SMA100 Series that could allow for arbitrary file deletion. 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. Successful exploitation of this vulnerability could result in arbitrary file deletion which enables an attacker to reboot the device to factory default settings. Afterwards, this could allow an unauthorized attacker to potentially gain admin access on the device. Depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

**THREAT INTELLIGENCE:**

There are currently no reports of this vulnerability being exploited in the wild.

**SYSTEMS AFFECTED:**

- SonicWall SMA 100 Series 9.0.0.10-28sv and earlier
- SonicWall SMA 100 Series 10.2.0.7-34sv and earlier
- SonicWall SMA 100 Series 10.2.1.0-17sv 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:**

A vulnerability has been discovered in the SonicWall SMA 100 Series that could allow for arbitrary file deletion. The improper access control vulnerability in SMA100 allows a remote unauthenticated attacker to bypass the path traversal checks and delete an arbitrary file potentially resulting in a reboot to factory default settings.

Successful exploitation of this vulnerability could allow an unauthorized attacker to potentially gain admin access on the device. Depending on the privileges associated with the application, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

**RECOMMENDATIONS:**
The following actions should be taken:

- 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:**
**SonicWall:**
https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0021

**CVE:**
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20034

**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.