*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**
**Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.**
**http://www.us-cert.gov/tlp/**

**DATE(S) ISSUED:**
02/04/2021

**SUBJECT:**
A Vulnerability in SonicWall SMA 100 Series Could Allow for SQL Injection

**OVERVIEW:**
A vulnerability has been discovered in the SonicWall SMA 100 Series, which could allow for SQL injection. 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 SQL injection, which enables the retrieval of admin credentials. Afterwards, this retrieval can pivot into a remote-code execution attack. 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 reports of this vulnerability being exploited in the wild as per NCCGroup.

**SYSTEMS AFFECTED:**
- SonicWall SMA 200, SMA 210, SMA 400, SMA 410
- SonicWall SMA 500v (Azure, AWS, ESXi, HyperV)

**RISK:**
**Government:**
- Large and medium government entities: **High**
- Small government entities: **High**

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

**Home users: Low**

**TECHNICAL SUMMARY:**
A vulnerability has been discovered in the SonicWall SMA 100 Series, which could allow for SQL injection. The improper SQL command neutralization in the SonicWall SSLVPN SMA100 product enables the execution of SQL commands of the attacker's choosing.

Successful exploitation of this vulnerability could result in SQL injection, which enables the retrieval of admin credentials. Afterwards, this retrieval can pivot into a remote-code execution

attack. 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:

- Apply the patched version of the SMA 10.x firmware to vulnerable systems immediately after appropriate testing.
- Apply appropriate countermeasures recommended by SonicWall within their advisory
- Apply the Principle of Least Privilege to all systems and services.

**REFERENCES:**
**SonicWall:**
https://www.sonicwall.com/support/product-notification/urgent-patch-available-for-sma-100-series-10-x-firmware-zero-day-vulnerability-updated-feb-3-2-p-m-cst/210122173415410/
https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001

**NCCGroup:**
https://twitter.com/NCCGroupInfosec/status/1355850304596680705