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
www.cisa.gov/tlp
Information may be distributed without restriction, subject to standard copyright rules.

DATE(S) ISSUED:
05/16/2022

SUBJECT:
Multiple Vulnerabilities in SonicWall SSLVPN SMA1000 Series Could Allow for Authentication Bypass

OVERVIEW:
Multiple vulnerabilities in SonicWall SMA 1000 Series could allow for authentication bypass. Successful exploitation could allow an attacker to have unauthorized access to internal resources and even redirect potential victims to malicious websites. The SonicWall SMA 1000 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.

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

SYSTEMS AFFECTED:

- SonicWall SMA 1000 Series Firmware versions between 12.4.0 and 12.4.1

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:

Multiple vulnerabilities in SonicWall SMA 1000 Series could allow for authentication bypass.

Tactic: Persistence (TA0003)

Technique: Modify Authentication Process (T1556)

- SMA1000 series appliance incorrectly restricts access to a resource from an unauthorized actor leading to Improper Access Control vulnerability. (CVE-2022-22282)

Tactic: Persistence (TA0009)

Technique: Browser Session Hijacking (T1185)

- Use of a shared and hard-coded encryption key (CVE-2022-1701)
- SMA1000 series appliances accept a user-controlled input that specifies a link to an external site and uses that link in a redirect which leads to Open redirection vulnerability. (CVE-2022-1702)

Successful exploitation of these vulnerabilities could allow for authentication bypass. This could allow an attacker to have unauthorized access to internal resources and even redirect potential victims to malicious websites.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by SonicWall to vulnerable systems immediately after appropriate testing. (M1051: Update Software)
    - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
    - **Safeguard 7.5: Perform Automated Vulnerability Scans of Internal Enterprise Assets:** Perform automated vulnerability scans of internal enterprise

assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.

- Block external access at the network boundary, unless external parties require service. (M1035: Limit Access to Resource Over Network)
    - **Safeguard 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure:** Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 12.3: Securely Manage Network Infrastructure:** Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.
- 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. (M1026: Privileged Account Management)
    - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
    - **Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts:** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.
- Deploy network intrusion detection systems to monitor network traffic for malicious activity.
    - **Safeguard 13.3: Deploy a Network Intrusion Detection Solution:** Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service.
    - **Safeguard 13.6: Collect Network Traffic Flow Logs:** Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.

REFERENCES:

CVE(s):https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22282

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1701

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1702

SonicWall:https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0009