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:
03/25/2022

SUBJECT:
A Vulnerability in SonicOS Could Allow for Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in SonicOS which could allow for remote code execution. SonicOS is the operating system for SonicWall network security appliances. Successful exploitation of this vulnerability could allow for an unauthenticated attacker to cause Denial of Service (DoS) or remote code execution on the firewall.

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

SYSTEMS AFFECTED:

- TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W, TZ570P, TZ670, NSa 2700, NSa 3700, NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, NSsp 13700, NSv 270, NSv 470, NSv 870 version 7.0.1-5050 and older
- NSsp 15700 version 7.0.1-R579 and older
- NSv 10, NSv 25, NSv 50, NSv 100, NSv 200, NSv 300, NSv 400, NSv 800, NSv 1600 version 6.5.4.4-44v-21-1452 and older

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 SonicOS which could allow for remote code execution. A stack-based buffer overflow could allow a remote unauthenticated attacker to send a specially crafted HTTP request to the targeted system and execute arbitrary code. Successful exploitation of this vulnerability could allow for an unauthenticated attacker to cause Denial of Service (DoS) or remote code execution on the firewall.

RECOMMENDATIONS:

We recommend the following actions 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:

SonicWall:https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0003

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22274