*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:**

04/21/2021

**SUBJECT:**

Multiple Vulnerabilities in SonicWall Email Security Could Allow for Arbitrary Code Execution

**OVERVIEW:**

Multiple vulnerabilities in SonicWall Email Security (ES) could allow for arbitrary code execution. Successful exploitation of these vulnerabilities could allow for arbitrary code execution. SonicWall Email Security (ES) is an email security solution that provides comprehensive inbound and outbound protection, and defends against advanced email-borne threats such as ransomware, zero-day threats, spear phishing and business email compromise (BEC). The solution can be deployed as a physical appliance, virtual appliance, software installation, or a hosted SaaS solution. 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:**

These vulnerabilities are currently being exploited in the wild. These vulnerabilities were chained to obtain admin rights and code execution capabilities on an on-premise SonicWall Email Security device.

**SYSTEMS AFFECTED:**

- SonicWall Email Security (ES) Versions 10.0.1-.4 - Present
- SonicWall Hosted Email Security (HES) Versions 10.0.1-.4 - Present

**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 have been discovered in SonicWall Email Security (ES) that could allow for arbitrary code execution. These vulnerabilities can be exploited using a chain style attack which is included in the below vulnerabilities:

- A pre-authentication admin account creation vulnerability that could enable a malicious actor to create an admin account by sending a specially crafted HTTP request to the remote host (CVE-2021-20021)
- A post-authentication arbitrary file creation vulnerability whereby a post-authenticated attacker could upload an arbitrary file to the remote host (CVE-2021-20022)
- A post-authentication arbitrary file read vulnerability whereby an attacker could read an arbitrary file from the remote host (CVE-2021-20023)

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-2021-20021
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20022
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20023

**FireEye:**
https://www.fireeye.com/blog/threat-research/2021/04/zero-day-exploits-in-sonicwall-email-security-lead-to-compromise.html

**SonicWall:**

https://www.sonicwall.com/support/product-notification/security-notice-sonicwall-email-security-zero-day-vulnerabilities/210416112932360/

**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.