SECURITY ALERT

# Cyber Defense Intelligence

January 25, 2022

**SECURITY ALERT:** Attackers continue to target Sonic Wall SMA critical vulnerability.

## Overview:

A critical vulnerability (CVE-2021-20038) affecting SonicWall's Secure Mobile Access (SMA) gateway was discovered yesterday. The vulnerability is an unauthenticated stack-based buffer overflow which impacts SMA 100 series appliances (including SMA 200, 210, 400, 410, and 500v). The vulnerability was addressed by SonicWall in December 2021, but attackers are still targeting the gateway.

Exploitation of CVE-2021-20038 allows remote unauthenticated attackers to execute code as the 'nobody' user in compromised SonicWall appliances. The vulnerability has a Common Vulnerability Scoring System score (CVSS) of 9.8 and allows attackers to overwrite several security-critical data on an execution stack that can lead to arbitrary code execution. CVE-2021-20038 could allow attackers to get complete control of a device or virtual machine. After gaining control, they would have the capability of installing malware to intercept authentication material from authorized users.

The issue found in the device stems from its web server - a slightly modified version of the Apache httpd server. Additionally, attackers are also trying to brute force their way in by password spraying known SonicWall appliance default passwords. There aren't any temporary mitigations for the vulnerability, so SonicWall urges customers to apply patches as soon as possible. This vulnerability affects versions 10.2.1.1-19sv, 10.2.0.8-37sv, and 10.2.1.2-24sv. SonicWall stated that they are actively monitoring activity against CVE-2021-20038 and urges all organizations regardless of security products to be consistent and thorough with their patching policy and execution.

**Indicators of Compromise (IoCs):**

At this time, there are no known IoCs.

**Pillar Technology Partners's Recommendations:**

SonicWall SMA 100 users are recommended to log in to their MySonicWall.com accounts to upgrade the firmware versions SonicWall outlined in their advisory.

Patch all devices. Please go to SonicWall's security advisory for details.

Due to password spraying, please change your passwords to strong/hard passwords

Monitor network traffic regularly

Provide training for IT staff on how to handle IoT medical devices

**References:**

Critical SonicWall NAC Vulnerability Stems from Apache Mods | Threatpost

Attackers now actively targeting critical SonicWall RCE bug (bleepingcomputer.com)

CVE-2021-20038..42: SonicWall SMA 100 Multiple Vulnerabilities (FIXED) | Rapid7 Blog

Security Advisory (sonicwall.com)