CyberSOC Threat Notification

SonicWall Zero-Day Vulnerability

Executive Summary

On February 1st, 2021 SonicWall released an updated security advisory confirming a zero-day vulnerability in their Secure Mobile Access (SMA) 100 series 10.x code. The flaw was reported by NCC Group on January 31st, 2021.

Description

On January 22nd, 2021, SonicWall disclosed that they suffered an attack on their internal systems which was likely caused by a zero-day vulnerability in certain SonicWall networking devices. SonicWall has confirmed that a critical zero-day vulnerability was discovered and has identified the vulnerable code. SonicWall firewalls, VPN clients, and SMA 1000 series appliance are unaffected by this flaw. NCC Group revealed that they detected an exploit being used against SonicWall SMA 100 devices in the wild.

Affected Products

- Physical and Virtual SMA 100 10.x devices
  - SMA 200
  - SMA 210
  - SMA 400
  - SMA 410
  - SMA 500v

Safeguards/Recommendations

SonicWall is currently developing a patch that is expected to be released by end of the day February 2, 2021. The security advisory includes a workaround which users can apply until a patch becomes available.

Version History

Version 1. Initial Report

Vendor: SonicWall

CVE-ID: N/A

Published: February 1, 2021

Patch Availability: No

Vulnerability Type: Zero-Day

Confidence Metrics

Remediation Level: Workaround

Report Confidence: High

Contact Us

24x7 SOC Phone: 215.867.9051
Email: soc@sra.io
Website: https://sra.io