VULNERABILITY BULLETINS

UPDATE: SonicWall SMA 100 Series Product Zero-Day Vulnerability

TLP:WHITE

Feb 04, 2021

*This updated alert provides details regarding a **zero-day vulnerability** for SMA 100 devices with 10.x firmware highlighting updated SNWLID-2021-0001 vulnerability information, upgrade recommended steps, and additional mitigation steps. In addition to the update, you may access the original Health-ISAC Vulnerability Bulletin here.*

*On February 3, 2021 SonicWall announced the availability of an SMA 100 series firmware 10.2.0.5-29sv update to patch a zero-day vulnerability on SMA 100 series 10.x code. To avoid potential exploitation, all SMA 100 series users must apply this patch **immediately**.*

Summary:

On January 31, 2021, a third-party threat research team from the NCC Group informed the SonicWall Product Security Incident Response Team (PSIRT) about a zero-day vulnerability affecting the Secure Mobile Access (SMA) 100 series product. Subsequently, the SonicWall security and engineering teams confirmed the vulnerable code and have begun working on a patch to be available by the end of the day. The SMA 100 series product provides an organization's employees with remote access to internal resources in which the vulnerability impacts only devices with firmware version 10.x.

The vulnerability is being tracked by SonicWall as *SNWLID-2021-0001* and affects both physical and virtual SMA 100 10.x devices including SMA 200, SMA 210, SMA 400, SMA410, and SMA500v. According to security research firm NCC Group, they detected an indiscriminate use of an exploit in the wild. The disclosure of this information corroborates with an earlier version of the SonicWall advisory. The advisory states that researchers identified a coordinated attack on its internal systems by highly sophisticated threat actors exploiting probable zero-day vulnerabilities on certain SonicWall secure remote access products.

Additional Web Application Firewall Mitigation Method

Customers unable to immediately deploy the patch can also enable the built-in Web Application Firewall (WAF) feature to mitigate the vulnerability in SNWLID-2021-0001 on SMA 100 series 10.x devices. Please follow guidance provided in the KB article to enable WAF functionality here. SonicWall is adding 60 complimentary days of WAF enablement to all registered SMA 100 series devices with 10.x code to enable this mitigation technique. Although the mitigation has been found to work, it does not replace the need to apply the patch in the long term and should only be used as a safety measure until the patched firmware is installed.

SonicWall is currently unaware of any forensic data that can be viewed by the user to determine whether a device has been attacked and will post updates accordingly. Vulnerable virtual SMA 100 series 10.x images have been pulled from AWS and Azure marketplaces and updated images will be submitted as soon as possible. During the interim, customers in Azure and AWS can update via incremental updates. Health-ISAC's Threat Operations Center (TOC) will continue to gather information regarding the submissions as they become available.

Reference(s)	Health-ISAC, SonicWall, mysonicwall, SonicWall, SonicWall, SonicWall

CVE(s)
CVE-2021-20016

CVSS Score
9.8

Recommendations

While SonicWall works to develop, test and release the patch, users may action the following options:

- If you must continue operation of the SMA 100 Series appliance until a patch is available

- Enable MFA as this is a critical step until the patch is available.
- Reset user passwords for accounts that utilized the SMA 100 series with 10.X firmware.

- If the SMA 100 series (10.x) is behind a firewall, block all access to the SMA 100 on the firewall.
- Shut down the SMA 100 series device (10.x) until a patch is available; or
- Load firmware version 9.x after a factory default settings reboot and make certain to back up your 10.x settings.

- Note: Direct downgrade of Firmware 10.x to 9.x with settings intact is not supported. You must first reboot the device with factory defaults and then either load a backed up 9.x configuration or reconfigure the SMA 100 from scratch.
- Ensure that you follow multifactor authentication (MFA) best practice security guidance if you choose to install 9.x.

SonicWall firewalls and SMA 1000 series appliances, as well as all respective VPN clients, are unaffected and remain safe to use.

Upgrade Recommended Steps

- Upgrade to SMA 10.2.0.5-29sv firmware, available here.

- This firmware is available for all users, regardless of the status of their support/service contract.
- Instructions on how to update the SMA 100 10.x series firmware for physical appliances and virtual devices can be found below:

- Physical Appliances
- Virtual Devices

- Reset passwords for any users who may have logged in to the device via the web interface.

- Enable multi-factor authentication (MFA) as a safety measure.

- MFA has an invaluable safeguard against credential theft and is a key measure of good security posture.
- MFA is effective whether it is enabled on the appliance directly or on the directory service in your organization.

NOTE: SMA 500v base image downloads from www[.]mysonicwall[.]com for Hyper-V, ESXi, Azure, AWS will soon be available.

Sources
SonicWall Product Notification

SonicWall Vulnerability List

Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Publication

Hackers Exploiting Critical Zero-Day in SonicWall Devices

Alert ID d4efa969

View Alert

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**