Urgent Update: SonicWall Confirms SMA 100 Series 10.X Zero-Day Vulnerability

LAST UPDATED: FEB. 1, 2021. 3 P.M. CST.

SonicWall has confirmed a zero-day vulnerability on SMA 100 series 10.x code. SMA 100 firmware prior to 10.x is unaffected by this zero-day vulnerability.

On Sunday, January 31, 2021, the NCC Group alerted the SonicWall Product Security Incident Response Team (PSIRT) about a potential zero-day vulnerability in the SMA 100 series. Our engineering team confirmed their submission as a critical zero-day in the SMA 100 series 10.x code. SonicWall believes it is extremely important to be transparent with our customers, our partners and the broader cybersecurity community and we are working around the clock to deliver a patch that will address the problem.

This vulnerability affects both physical and virtual SMA 100 10.x devices (SMA 200, SMA 210, SMA 400, SMA 410, SMA 500v). A few thousand devices are impacted.

While SonicWall works to develop, test and release the patch, organizations should follow the updated guidance located here: https://www.sonicwall.com/support/product-notification/210122173415410/
SonicWall firewalls and SMA 1000 series appliances, as well as all respective VPN clients, are unaffected and remain safe to use.

LAST UPDATED: JAN. 23, 2021. 9.45 P.M. CST.

SonicWall believes it is extremely important to be transparent in providing the latest information to our customers, partners and the broader cybersecurity community about the ongoing attacks on global business and government.

As an update to previous communication, SonicWall engineering teams continued their investigation into probable zero-day vulnerabilities and have produced the following update regarding the impacted products:

NOT AFFECTED

- **SonicWall Firewalls:** All generations of SonicWall firewalls are not affected by the vulnerability impacting the SMA 100. **No action is required from customers or partners.**

- **NetExtender VPN Client:** While we previously communicated NetExtender 10.x as potentially having a zero-day, that has now been ruled out. It may be used with all SonicWall products. No **action is required from customers or partners.**
- **SMA 1000 Series:** This product line is not affected by this incident. Customers are safe to use SMA 1000 series and their associated clients. **No action is required from customers or partners.**
- **SonicWave Access Points:** Not affected. **No action is required from customers or partners.**

REMAINS UNDER INVESTIGATION

- **SMA 100 Series:** This product remains under investigation. However, SMA 100 series products may be used safely in common deployment use cases. For details on these use cases and further mitigation steps, please read: https://www.sonicwall.com/support/product-notification/210122173415410.

For additional details, guidance and product usage, customers may reference the KB article, which we will continue to update throughout our investigation. SonicWall fully understands the challenges previous guidance had in a work-from-home environment, but the communicated steps were measured and purposeful in ensuring the safety and security of our global community of customers and partners.

ORIGINAL POST: JAN. 22, 2021. 10 P.M. CST.

SonicWall provides cybersecurity products, services and solutions that are designed to help keep organizations safe from increasingly sophisticated cyber threats. As the front line of cyber defense, we have seen a dramatic surge in cyberattacks on governments and businesses, specifically on firms that provide critical infrastructure and security controls to those organizations.

We believe it is extremely important to be transparent with our customers, our partners and the broader cybersecurity community about the ongoing attacks on global business and government.

Recently, SonicWall 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. The impacted products are:

- Secure Mobile Access (SMA) version 10.x running on SMA 200, SMA 210, SMA 400, SMA 410 physical appliances and the SMA 500v virtual appliance

The NetExtender VPN client and SMB-oriented SMA 100 series are used for providing employees/users with remote access to internal resources.

We are providing mitigation recommendations to our channel partners and customers. For further guidance, please visit: https://www.sonicwall.com/support/product-notification/210122173415410. We will continue to update this knowledge base (KB) article as more information is available.

MEDIA CONTACTS

Lindsey Lockhart
Director of Public Relations
T: +1 214 562 1521
llockhart@sonicwall.com