


# Additional SMA 100 Series 10.x and 9.x Firmware Updates Required [Updated April 29, 2021, 12:30 P.M. CST]

 [sonicwall.com/support/product-notification/urgent-security-notice-sonicwall-confirms-sma-100-series-10-x-zero-day-vulnerability-feb-1-2-p-m-cst/210122173415410/](https://sonicwall.com/support/product-notification/urgent-security-notice-sonicwall-confirms-sma-100-series-10-x-zero-day-vulnerability-feb-1-2-p-m-cst/210122173415410/)



## Update: April 29, 2021, 12:30 P.M. CST

SonicWall is announcing the availability of new firmware versions for both 10.x and 9.x code on the SMA 100 series products, comprised of SMA 200, 210, 400, 410 physical appliances and the SMA 500v virtual appliance.

### Upgrade Steps

All organizations using SMA 10.x or SMA 9.x firmware should immediately implement the following:

Upgrade to the latest SMA 100 series firmware available from [www.mysonicwall.com](http://www.mysonicwall.com).

SMA 100 series 10.x customers should upgrade to **10.2.0.7-34sv** firmware.

SMA 100 series 9.x customers should upgrade to **9.0.0.10-28sv** firmware.

*UPDATE: February 19, 2021, 2 P.M. CST*

Following up on the Feb. 3 firmware update outlined below, SonicWall is announcing the availability of new firmware versions for both 10.x and 9.x code on the SMA 100 series products, comprised of SMA 200, 210, 400, 410 physical appliances and the SMA 500v virtual appliance.

SonicWall conducted additional reviews to further strengthen the code for the SMA 100 series product line.

The new SMA 10.2 firmware includes:

- Code-hardening fixes identified during an internal code audit
- Rollup of customer issue fixes not included in the Feb. 3 patch
- General performance enhancements
- Previous SMA 100 series zero-day fixes posted on Feb. 3

The new 9.0 firmware includes:

Code-hardening fixes identified during an internal code audit

**SMA 100 Series Devices with 10.x or 9.x Firmware that Require Upgrade:**

- **Physical Appliances:** SMA 200, SMA 210, SMA 400, SMA 410
- **Virtual Appliances:** SMA 500v (Azure, AWS, ESXi, HyperV)

**All organizations using SMA 100 series products with 10.x or 9.x firmware** should apply the respective patches **IMMEDIATELY**.

If you already applied the SMA 10.2.0.5-29sv firmware posted on Feb 3., **you still need to upgrade to SMA 10.2.0.6-32sv**. If you skipped the SMA 10.2.0.5-29sv firmware update from Feb. 3, you only need to apply the latest SMA 10.2.0.6-32sv firmware.

**Upgrade Steps**

All organizations using SMA 10.x or SMA 9.x firmware should **immediately** implement the following:

1. Upgrade to the latest SMA 100 series firmware available from [www.mysonicwall.com](http://www.mysonicwall.com).
  - o SMA 100 series 10.x customers should upgrade to **10.2.0.6-32sv** firmware
  - o SMA 100 series 9.x customers should upgrade to **9.0.0.10-28sv** firmware
  - o Both firmware versions are available for **everybody**, regardless of the status of their support/service contract.
  - o Instructions on how to update the SMA 100 10.x or 9.x series firmware can be found in [this KB article for physical appliances](#) and [this KB article for virtual devices](#).
2. After applying the patch, reset passwords for any users who may have logged in to the device via the web interface. **This step only applies if you did not deploy the older SMA 10.2.0.5-29sv firmware update from Feb. 3.**
3. Enable multifactor authentication (MFA) as a safety measure.
  - o MFA has an invaluable safeguard against credential theft and is a key measure of good security posture.
  - o MFA is effective whether it is enabled on the appliance directly or on the directory service in your organization.
  - o For assistance enabling one-time passwords (OTP) on SMA 100, please review the KB article [How Can I Configure Time-Based One Time Password \(TOTP\) In SMA 100 Series?](#)

Release notes for both firmware can be found in the downloads section of [mysonicwall.com](http://mysonicwall.com).

*UPDATE: February 3, 2021, 2. P.M. CST*

SonicWall is announcing 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. All SMA 100 series users must apply this patch **IMMEDIATELY** to avoid potential exploitation.

### **Affected SMA 100 Devices with 10.x Firmware that Require the Critical Patch:**

- **Physical Appliances:** SMA 200, SMA 210, SMA 400, SMA 410
- **Virtual Appliances:** SMA 500v (Azure, AWS, ESXi, HyperV)

Please read this notice in its entirety as it contains important details for post-upgrade steps.


### **Vulnerability Information**

The patch addresses vulnerabilities reported to SonicWall by the NCC Group on Jan. 31 and Feb. 2, tracked under PSIRT Advisory ID [SNWLID-2021-0001](#). These include an exploit to gain admin credential access and a subsequent remote-code execution attack.

### **Upgrade Recommended Steps**

Due to the potential credential exposure in SNWLID-2021-0001, all customers using SMA 10.x firmware should immediately follow the following procedures:

1. Upgrade to SMA 10.2.0.5-29sv firmware, available from [www.mysonicwall.com](http://www.mysonicwall.com).
  - o This firmware is available for everybody, regardless of the status of their support/service contract.
  - o Instructions on how to update the SMA 100 10.x series firmware can be found in this [KB article for physical appliances](#) and this [KB article for virtual devices](#).
2. Reset the passwords for any users who may have logged in to the device via the web interface.
3. Enable multifactor authentication (MFA) as a safety measure.
  - o MFA has an invaluable safeguard against credential theft and is a key measure of good security posture.
  - o 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](http://www.mysonicwall.com) for Hyper-V, ESXi, Azure, AWS will be available shortly.

### **Additional WAF 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 the guidance in the following KB article to enable WAF functionality:  
<https://www.sonicwall.com/support/knowledge-base/210202202221923/>

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.

While this mitigation has been found in our lab to mitigate SNWLID-2021-0001, 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.

### **Additional Notes**

- We currently are not aware of any forensic data that can be viewed by the user to determine whether a device has been attacked. However, we will post an update as we get more information.

- Vulnerable virtual SMA 100 series 10.x images have been pulled from AWS and Azure marketplaces and updated images will be re-submitted as soon as possible. We expect the approval process to take several weeks. In the meantime, customers in Azure and AWS can update via incremental updates.

Release notes for the firmware can be found in the downloads section of [www.mysonicwall.com](http://www.mysonicwall.com)

*UPDATE: February 3, 2021, 6. A.M. CST*

SonicWall engineering teams continue to finalize the SMA 100 series 10.x patch that addresses the zero-day vulnerability.

**The new estimate for delivery is mid-day Feb. 3 (PST).**

Meanwhile, as outlined below, you can enable the built-in Web Application Firewall (WAF) functionality on the SMA 100 series appliance to help protect against the vulnerability. Please follow the guidance in the following KB article to enable WAF functionality on the SMA 100 series appliance: <https://www.sonicwall.com/support/knowledge-base/security-best-practice-for-configuring-web-application-firewall/210202202221923/>.

*UPDATE: February 2, 2021, 11. P.M. CST*

The SMA 100 series 10.x patch announced yesterday to address the zero-day vulnerability is still undergoing final testing and our **new estimate for delivery is early Feb. 3 (PST)**.

Meanwhile, we have identified an additional mitigation to remediate the attack on the SMA 100 series 10.x firmware. The built-in Web Application Firewall (WAF) functionality has been observed in our testing to neutralize the zero-day vulnerability. Please follow the guidance in the following KB article to enable WAF functionality on the SMA 100 series appliance: <https://www.sonicwall.com/support/knowledge-base/210202202221923/>

SonicWall is adding 60 complimentary days of WAF enablement to all registered SMA 100 series devices with 10.X code in order to enable this mitigation technique. This 60-day license will be automatically enabled within “www.MySonicWall.com” accounts of registered SMA 100 series devices before the end of today, Feb. 2 (PST).

The Feb. 3 patch remains the definitive solution to the zero-day vulnerability. The patch will include additional code-strengthening and should be applied immediately upon availability.

*UPDATE: February 1, 2021, 2.30 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](#) informed 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, and are tracking it as [SNWLID-2021-0001](#).

SonicWall has identified the vulnerable code and is working on a patch to be available by end of day on February 2, 2021. This vulnerability affects both physical and virtual SMA 100 10.x devices (SMA 200, SMA 210, SMA 400, SMA 410, SMA 500v).

While we work to develop, test and release the patch, customers have the following options:

1. If you must continue operation of the SMA 100 Series appliance until a patch is available
  1. Enable MFA. This is a **\*CRITICAL\*** step until the patch is available; AND
  2. Reset user passwords for accounts that utilized the SMA 100 series with 10.X firmware
2. If the SMA 100 series (10.x) is behind a firewall, block all access to the SMA 100 on the firewall;
3. Shut down the SMA 100 series device (10.x) until a patch is available; or
4. Load firmware version 9.x after a factory default settings reboot. **\*Please back up your 10.x settings\***
  1. **Important 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.
  2. 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.

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

*UPDATE: January 29, 2021, 5.30 P.M. CST*

As we head into the weekend, we continue to investigate the SMA 100 Series, however the presence of a potential zero-day vulnerability remains unconfirmed.

We have also analyzed several reports from our customers of potentially compromised SMA 100 series devices. In these cases, we have so far only observed the use of previously stolen credentials to log into the SMA devices. The SMA appliance, due to its nature and due to prevalence of remote work during the pandemic, effectively acts as a “canary” to raising an alert about inappropriate access. These specific cases came to light through, and were mitigated by, MFA or End Point Control (EPC). This **further emphasizes the importance of enabling these features**, not only on the SMA series, but across the entire enterprise as a generally recommended security practice. In the age of cloud services and remote work, credentials can be the key to the kingdom and attackers are keenly aware of this.

We’re also aware of social media posts that shared either supposed proof of concept (PoC) exploit code utilizing the Shellshock exploit, or screenshots of allegedly compromised devices. We have confirmed that the Shellshock attack has been mitigated by patches that we released in 2015. We have also tested the shared PoC code and have so far concluded that **it is not effective against firmware released** after the 2015 patch. However, we’ll continue to closely monitor any new posts and investigate new information. This should also serve as a reminder to our customer base **to always patch and keep current** on internet facing devices.

A reminder to our customers: SonicWall policy has always been to release firmware with vulnerability patches to everyone, regardless of the support status on the device in question. Therefore, even if you do not have a valid support contract on your SMA 100 series device, or any SonicWall device, you can download firmware up to the latest vulnerability fixes on [www.mysonicwall.com](http://www.mysonicwall.com). Please take advantage of these updates to ensure that your equipment is up to the latest firmware.

We will continue to fully investigate this matter and share more information and guidance as we have it. We will post further updates on this KB and will hopefully soon rule definitively on the outcome of this investigation.

We’ve also released an updated security best practices guide for the SMA 100 series devices, including instructions on how to enable MFA:

[SMA 100 Series Security Best Practice Guide](#)

*UPDATE: January 29, 2021. 7 A.M. CST.*

SonicWall security and engineering teams remain focused on the incident and have no updates to share at this time. We fully understand the urgency of the matter and will continue to communicate updates in this KB article.

We're also publishing a new guide on enabling multifactor authentication (MFA) on SMA 100 series appliances to assist those following best practices. This will be available on our website later today. The previous guidance outlined below also remains in effect.

*UPDATE: January 27, 2021. 7 P.M. CST.*

We continue to investigate the incident and have no further updates to share at this time. Please continue to roll out MFA protection per best-practice guidance across your remote user base.

Additionally, we continue to receive questions about older versions of NetExtender. We want to clarify that NetExtender 10.x and prior versions are not impacted in this incident.

Best practice guidance outlined below remains in effect and has not changed.

*UPDATE: January 25, 2021. 5.30 P.M. CST.*

SonicWall engineering teams continue their investigation into probable zero-day vulnerabilities with SMA 100 series products. SonicWall fully understands the urgency for information and guidance, which we're committed to providing as we verify and confirm details. Below is updated guidance for SMA 100 series products. These steps should be adhered to until our next update.

#### NOT AFFECTED

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

#### REMAINS UNDER INVESTIGATION

**SMA 100 Series:** The SMA 100 series (SMA 200, SMA 210, SMA 400, SMA 410, SMA 500v) remains under investigation for a vulnerability. However, we can issue the following guidance on deployment use cases:

Current SMA 100 series customers may continue to **safely use NetExtender for remote access** with the SMA 100 series. We have determined that this use case is not susceptible to exploitation.

**IMPORTANT:** At this time, it is **critical** that organizations with active SMA 100 Series appliances take the following action:

Enable two-factor authentication (2FA) on SMA 100 series appliances

Please refer to the following knowledgebase article:

<https://www.sonicwall.com/support/knowledge-base/how-can-i-configure-time-based-one-time-password-totp-in-sma-100-series/180818071301745/>

In addition to implementing 2FA, SMA 100 series administrators may also consider the following to further secure access to these devices:

- Enable Geo-IP/botnet filtering and create a policy blocking web traffic from countries that do not need to access your applications.  
See page 248 of the [SMA 100 Series 10.2 Administration Guide](#)
- Enable and configure End Point Control (EPC) to verify a user's device before establishing a connection.  
See page 207 of the [SMA 100 Series 10.2 Administration Guide](#)
- Restrict access to the portal by enabling Scheduled Logins/Logoffs  
See page 117 of the [SMA 100 Series 10.2 Administration Guide](#)

Please refer to the SonicWall issued PSIRT Advisory [SNWLID-2021-0001](#) for updates. As we continue to investigate the incident, we will provide further updates regarding mitigation or possible patches in this KB.

*UPDATE: January 23, 2021, 9:30 P.M. CST.*

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 series (SMA 200, SMA 210, SMA 400, SMA 410, SMA 500v). 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.
- **SonicWall SonicWave APs:** No action is required from customers or partners.

#### REMAINS UNDER INVESTIGATION

**SMA 100 Series:** This product remains under investigation for a vulnerability, however we can issue the following guidance on deployment use cases:

- Current SMA 100 Series customers **may continue to use NetExtender for remote access** with the SMA 100 series. We have determined that this use case is not susceptible to exploitation.
- We advise SMA 100 series administrators to create specific access rules or disable Virtual Office and HTTPS administrative access from the Internet while we continue to investigate the vulnerability.

As we continue to investigate the incident, we will provide further updates in this KB.

*UPDATE: January 22, 2021. 10:15 P.M. CST.*

SonicWall provides cybersecurity products, services and solutions 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:

- **NetExtender VPN client version 10.x (released in 2020) utilized to connect to SMA 100 series appliances and SonicWall firewalls**
- **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. The SMA 1000 series is not susceptible to this vulnerability and utilizes clients different from NetExtender.

**IMPORTANT:** Organizations with active SMA 100 Series appliances or with NetExtender 10.x currently have the following options:

For SMA 100 Series

- Use a firewall to only allow SSL-VPN connections to the SMA appliance from known/whitelisted IPs
- Or configure whitelist access on the SMA directly itself
- Please reference:

<https://www.sonicwall.com/support/knowledge-base/how-to-restrict-access-for-netextender-mobile-connect-users-based-on-policy-for-ip-address/170502499350337/>

For Firewalls with SSL-VPN access via NetExtender VPN Client Version 10.x

- Disable NetExtender access to the firewall(s) or restrict access to users and admins via an allow-list/whitelist for their public IPs
- Please reference:

<https://www.sonicwall.com/support/knowledge-base/how-do-i-configure-the-ssl-vpn-feature-for-use-with-netextender-or-mobile-connect/170505401898786/>

MFA Must Be Enabled on ALL SonicWall SMA, Firewall & MySonicWall Accounts