CU*ANSWERS
A Credit Union Service Organization

6000 28TH STREET S.E. • GRAND RAPIDS, MI 49546
phone: 616.285.5711 • 800.327.3478 • fax: 616.285.5735
visit us on the web: www.cuanswers.com

March 15, 2021

To: CU*Answers SonicWall Clients

From: CU*Answers Executive Team
CU*Answers Network Services
CU*Answers Disaster Recovery/Business Resumption
CU*Answers Internal Audit

Re: SonicWall Vulnerability Close Out Report

PURPOSE

This report is a recap of CU*Answers actions and strategy surrounding a series of announcements from SonicWall regarding vulnerabilities in their client (PC) VPN products and platforms. This report is intended to summarize CU*Answers' actions and strategy regarding the vulnerabilities and mitigation steps taken. This report can be provided to our clients' Board of Directors and examiners as part of their due diligence process.

At the time of this report, there is no evidence that CU*Answers or any managed client using SonicWall products were compromised or breached as a consequence of this vulnerability. Should CU*Answers discover evidence of compromise in the future, CU*Answers will notify clients in accordance with regulatory requirements and its contractual obligations.

Our Teams welcome feedback from our clients. CU*Answers looks forward to hearing from our cooperative partners regarding any questions, concerns, or assistance on managing any future security incidents.

INCIDENT SUMMARY

The announcements that SonicWall had a security vulnerability affected both CU*Answers internally and our managed clients. Therefore, CU*Answers teams were required to manage both internal and client systems. CU*Answers generally took a conservative approach with respect to possible risk. There were no significant issues by either internal staff or clients regarding CU*Answers security posture and mitigation.

This incident had four major phases:

Initial Announcement and Mitigation. CU*Answers disabled NetExtender access internally and for clients. CU*Answers implemented whitelisting to allow only approved IP address to connect to the VPN systems for our clients. Changes for clients were tracked in the CU*Answers ticketing system.

Coordination with Partners and Clients. The next week was spent ensuring all clients were aware of the situation and agreed with the mitigation steps as performed by CU*Answers.

Announcement of Mobile Access Vulnerability, and Mitigation. CU*Answers was informed by SonicWall that mobile access had a zero-day vulnerability for mobile email access. CU*Answers rolled these mobile email systems back to a previous version not affected by the vulnerability. Systems were patched as soon as the update was made available by SonicWall. This included a second patch to help harden the platform released approximately a week later.

Rollback to Previous Functionality. After patching, and after more than a week of observation and assessment, CU*Answers developed a plan to roll internal and client systems back to previous functionality, and to end the administrative burden of the whitelisting mitigation strategy.

Details on each phase and mitigation steps follow. Announcements made to clients and our internal staff are *italicized* for reference.

JANUARY 23-24: INITIAL ANNOUNCEMENT AND RESPONSE

On Saturday, January 23 SonicWall announced a significant vulnerability in its VPN NetExtender and Secure Mobile Access VPN client (PC) products. SonicWall advised, among other mitigation steps, to disable NetExtender access to the firewall. This kicked off several weeks of mitigation steps for CU*Answers and our clients.

Per our Security Response Protocol, the CU*Answers Incident Team met that evening to discuss options in light of the information provided by SonicWall. For CU*Answers internal users:

1. Network Services disabled NetExtender access at CU*Answers on the gr.cuanswers.com and kwd.cuanswers.com remote access appliances.

2. Bookmarks, functionality that allowed users to log into their office machines via web portal were not impacted.

3. An announcement to staff was made for alternative access for critical team members. DR/BR helped with coordination with the management team to identify critical employees. Capacity was analyzed to ensure enough licenses were available for critical team members. Instructions were sent to staff if they needed to change connectivity.

Network Services notified managed clients and disabled affected systems for them as well. The following notification was sent Saturday January 23:

> *On Saturday, January 23 SonicWall announced a significant vulnerability in its NetExtender service, which runs on both firewalls and security mobile access appliances. SonicWall advised, among other mitigation steps, to disable NetExtender access.*
>
> *As part of CU*Answers incident response protocol, CU*Answers is following the recommendations from SonicWall for both our own network and for clients we manage by disabling NetExtender functionality. This will result in service outages for personal VPN connections using NetExtender. Connections using remote desktop bookmarks, Outlook Mobile Access should continue to function normally.*
>
> *This change should not have any impact on network connectivity as a whole, nor the other security functionality provided by the SonicWall appliances.*
>
> *While there is no evidence that any network managed by us has been compromised as a result of this vulnerability, our security protocol dictates eliminating vulnerable systems until remediated.*
>
> *CU*Answers will update clients and provide an update on the restoration of SonicWall personal VPN services no later than Monday, January 25, noon EST.*
>
> *If you need weekend support for critical remote access functions that have been disabled, please call our after-hours support at 800.327.3478 and we will arrange for a technician to reach out and assist.*
>
> *You can read more about the vulnerability here:*
>
> *https://www.sonicwall.com/support/product-notification/urgent-security-notice-netextender-vpn-client-10-x-sma-100-series-vulnerability/210122173415410/*

CU*Answers approach to managing clients for the initial announcement and mitigation steps were as follows:

1. The ticketing system was used to manage client tracking.

2. Primary mitigation strategy was whitelisting client VPN IP addresses. Whitelisting only allows approved IP addresses to access the affected devices. Network Services made changes to around 200 devices.

3. In addition, dedicated support was lined up for Monday, January 25. Laura Welch-Vilker made arrangements for the CSR team to help triage remote support calls, and Jim Lawrence helped organize Ops' responses for Sunday calls.

On the same day, SonicWall sent out an update that contradicted their first announcement. This new announcement stated that VPN NetExtender products were not affected by the vulnerability.

CU*Answers made the decision to keep the same security posture and advised clients as such in the following communication on Sunday, January 24:

> *On Saturday, January 23, SonicWall announced a vulnerability to their client VPN NetExtender and SMA products, along with mitigation steps. Later that same evening, SonicWall published an update stating these products were not actually affected.*
>
> *Although there was no evidence of any compromise, CU*Answers had already begun mitigation for our own network and our managed clients at the time the all-clear message came from SonicWall. Despite the latest SonicWall statement, CU*Answers is maintaining its mitigation security posture for the time being. Our Network Services Team has also reached out to SonicWall for additional clarification.*
>
> *If your credit union uses SonicWall VPN products not managed by CU*Answers, we recommend you review SonicWall's announcement and updates. If your credit union's NetExtender VPN is managed by CU*Answers, we have already taken mitigation steps. You can contact our Network Services Team if you need any additional information on the mitigation process.*
>
> *You can read SonicWall's latest update here: https://www.sonicwall.com/support/product-notification/urgent-security-notice-netextender-vpn-client-10-x-sma-100-series-vulnerability-updated-jan-23-2021/210122173415410/*

Network Services also reached out personally to clients to update them on the announcement and CU*Answers security posture. Network Services coordinated with internal staff to ensure no downtime for CU*Answers on Monday, January 25.

WEEK OF JANUARY 25: COORDINATION WITH PARTNERS AND CLIENTS

The CU*Answers Team continued to press SonicWall for additional information during the first week after the announcement. Updates were provided to clients regarding CU*Answers' discussions with SonicWall. CU*Answers considered several alternative solutions during this week, including migrating to a new solution or developing a new one. Ultimately, CU*Answers chose to stay the course and continue with whitelisting and other mitigation tactics.

> *By 5PM Wednesday, January 27, CU*Answers had reached out to most affected clients and partners, including CU*South and CU*NorthWest. No clients asked to have CU*Answers deviate from its mitigation strategy. The primary challenge for clients were those that had dynamic IP addresses. Dynamic IP address constantly change, so it was virtually impossible for the team to whitelist these IP addresses.*

Due to a lack of substantive updates from SonicWall, CU*Answers sent the following update on the morning of February 1:

> *CU*Answers continues to actively monitor the SonicWall situation. No new or actionable information has been made available at this time.*

*CU*Answers intends to maintain our current security posture and mitigation strategy for both managed clients and our own network.*

If your credit union is affected, please contact our Network Services Team. We have established an approach to mitigate the risk of the vulnerability and to re-enable these services. The mitigation requires whitelisting source IP information for your remote users. While this approach should allow us to enable remote access for many, it will not work for all and may require additional support if the remote user's IP address changes.

If you need support for remote access functions that have been disabled, please call the CNS team at 800.327.3478 or email us at helpdesk@cuanswers.com. We have dedicated team members standing by to provide support. Please have a list of users by priority that need access and that will be able to test.

CU*Answers also provided to clients the latest SonicWall updates. However, shortly thereafter SonicWall did come out with an announcement that required CU*Answers to take additional mitigation steps.

FEBRUARY 1-2: ZERO DAY VULNERABILITY ANNOUNCED IN SONICWALL'S SMA (SECURE MOBILE ACCESS) PLATFORM

Late afternoon on February 1, SonicWall provided an update confirming a zero-day vulnerability in its SMA platform. Because this was a new announcement, the CU*Answers Incident Response Team reconvened that evening to review the finding, correspond with SonicWall senior management, and identify potential areas of exposure. For CU*Answers internal users, the team reviewed and took the following steps:

1. Network Services shut down the SMA system immediately as no IP whitelisting was in place for that system. About 50 CU*Answers users in total affected.

2. CU*Answers users were migrated to the my365 environment. Notification to users was coordinated through the DR/BR notification system.

3. Support resources were marshalled for the morning of February 2 in the remote support queue.

4. All network passwords were reset for all users of those portals back to January 1.

The message sent to CU*Answers employees through the emergency notification system was as follows:

*ATTN: CU*Answers will be shutting down remote to desktop access tonight in response to the evolving SonicWall VPN issue. We have setup alternate access via https://my365.cuanswers.com. Because we need to conserve licenses, please refrain from*

utilizing this link unless you are doing emergency work or are a full-time remote worker. Please contact CNS VPN support tomorrow at x104 for assistance.

Network Services also reviewed mitigation steps in light that some cooperative client SMAs were affected:

1. Roughly 25 client devices were affected. SonicWall confirmed that the IP whitelisting by the firewall is a good mitigation tactic.

2. Network Services contacted all affected clients in the morning to reset remote user credentials.

3. Network Services reviewed all client setup to ensure MFA is enabled.

4. Support resources were notified of the internal and external situation and were asked to be ready in the morning.

Finally, the SonicWall announcement implied Outlook Mobile Access (i.e., email to phones) may be affected. Risk to these devices was unknown but not denied by SonicWall. However, CU*Answers had no evidence any devices were compromised based on a lack of attacker behavior. Therefore, CU*Answers took the following steps:

1. On the night of February 1, device quarantine was investigated, meaning that any new devices connecting would require admin approval.

2. CU*Answers would look to mitigate by rolling the system back to an earlier version of the operating system that did not have the vulnerability.

The CU*Answers Incident Team working with our Executive Team made the decision on February 2 to take the SMA systems offline during the day to apply the patch. The following email was sent to internal CU*Answers staff:

Team,

*In response to the evolving security issue with some SonicWall equipment, CU*Answers will be disabling all mobile device email syncing from approximately 11:00 AM until 1:30 PM today to apply mitigating software to our mobile device gateway.*

- *This means email and calendar events will not sync with your mobile device during the time of this maintenance period.*

- *Notifications of this maintenance will also be sent via our EMS text service.*

- *This work does not affect clients.*

- *Only users of mobile email at CU*Answers, CU*South, CU*Northwest, eDOC, and Xtend will be affected.*

- *This work does not affect employee remote access VPNs.*

- *Mobile email users may need to restart their email applications after the work completes in order to resume syncing.*

- *If you experience issues with email syncing after the maintenance completes, please contact the CNS Help Desk at x266.*

Next Steps:

1. *After this maintenance completes and in an abundance of caution, we will be sending another notification requesting users change their network passwords as soon as practical. CNS will monitor compliance and will contact users individually as necessary.*

2. *Within the next week, we will conduct follow up maintenance on the mobile email gateway, which will result in another outage period. We will announce those details and dates when we have them.*

The appliance was moved to the previous version of the O/S and tested by 1:14PM Eastern Time.

Network Services also worked with the smaller subset of clients that might be affected to review previously implemented mitigation strategies. CU*Answers recommended that SMA users change their passwords as soon as possible as an additional precaution. CU*Answers had no evidence of compromised credentials and has been following the guidance to mitigate the vulnerability by whitelisting user IP addresses.

FEBRUARY 3-15: NEW FIRMWARE UPDATE AND CLIENT COMMUNICATIONS

On February 3, SonicWall released a firmware update (patch) for affected systems. The CU*Answers Incident Team met to discuss options. The decision was made to patch systems and maintain the same security posture, observing performance and evaluating the security risks.

The following update to clients was sent by Network Services:

Update:

Today SonicWall released more information on mitigation of the remote access vulnerability. SonicWall has also released a firmware update that they are recommending be applied immediately to affected units.

SonicWall has confirmed that this vulnerability affects only SMA 100 series equipment.

*Please note this update and vulnerability only affect a small subset of the clients we initially notified. We are scheduling patch installation for all affected clients starting this evening. If you have SMA 100 series equipment managed by CU*Answers we will apply the patch tonight.*

We will open a ticket to notify you of the patch installation and to confirm when its complete. If you do not see a ticket it means you do not have hardware that is affected.

In addition to applying this firmware, SonicWall is recommending that all remote access users reset their passwords. We will provide a list of those users and assistance with completing this process tomorrow.

Additionally, we recommend keeping all complementary security controls in place, including IP whitelisting and multifactor authentication.

If you have any questions please contact us: helpdesk@cuanswers.com

Firmware updates were applied to internal and client systems by February 4. CU*Answers continued to maintain the same security posture, observation, and pressing SonicWall for further details and updates.

FEBRUARY 15-17: ROLL BACK TO FULL FUNCTIONALITY

In the absence of any additional information, and a lack of pushback from clients on patch effectiveness, the CU*Answers Incident Response Team proposed that the Executive Team approve a plan to move back to full functionality. The CU*Answers Executive Team agreed.

1. CU*Answers' planned to update the SMA for staff with full functionality this week, and update and patch the mobile email appliance Wednesday, February 17 between 2-4AM.

2. NetExtender, which SonicWall ruled out as having issues, had whitelists removed unless clients requested otherwise (the administrative maintenance load for whitelists is high).

Network Services completed this plan and updated clients with the following communication:

Update:

It has been 13 days since SonicWall released the 100 series zero-day vulnerability patch.

If your equipment was affected, a ticket was opened and the update applied on 2/4/2021. If you did not see a ticket, your equipment was not affected.

Since the patch release there have been no further updates from SonicWall and no feedback from the cybersecurity community regarding other vulnerabilities or patch efficacy.

We are re-enabling remote access functionality on all managed equipment that was previously disabled. As with the patch application, you will see a ticket opened for your organization to track the work.

We are also removing any IP whitelisting configurations to restore functionality to those affected. If you wish to keep your whitelist in place, please let us know.

If you have any questions please contact us: helpdesk@cuanswers.com

FEBRUARY 24: FINAL STATEMENT FROM SONICWALL

On February 24, SonicWall issued essentially their final statement about the events of January and February. In summary:

- SonicWall first issued a zero-day vulnerability alert for one of our remote access products, the SMA 100 series, which we now believe was used in the attack.

- SonicWall's investigation in consultation with forensic experts concluded there is no evidence that any other SonicWall products are impacted or that SonicWall's source code has been modified or otherwise compromised.

- SonicWall is conducting additional third-party code reviews.

- SonicWall admitted the January incident resulted in the exfiltration of some limited internal SonicWall files. Impacted parties and relevant regulators have been notified of this event.

A copy of this announcement is available at the end of this report.

APPENDIX: FEBRUARY 24 ANNOUNCEMENT BY SONICWALL

SONICWALL

As previously communicated, SonicWall was the target of an attack by a highly sophisticated threat actor in mid-January. SonicWall's priority in responding to the attack was identifying, resolving and providing alerts regarding potential product vulnerabilities that could impact our customers.

SonicWall first issued a zero-day vulnerability alert for one of our remote access products, the SMA 100 series, which we now believe was used in the attack. On Feb. 3 we released a critical patch for the vulnerability, and on Feb. 19 we issued an update with additional code-hardening for the SMA 100 series product line.

Based on our extensive investigation in consultation with forensic experts, there is no evidence that any other SonicWall products are impacted or that SonicWall's source code has been modified or otherwise compromised. As a precaution, we are conducting additional third-party code reviews to supplement the standard code audits that are part of our development and PSIRT processes.

The January incident resulted in the exfiltration of some limited internal SonicWall files. Impacted parties and relevant regulators have been notified of this event.

We appreciate the support and confidence shown by our partners and customers as we have worked through the stages of this event and the ensuing investigation.

SonicWall remains committed to delivering world-class cybersecurity solutions for our partners and customers, and we will continue to communicate the latest information and guidance for keeping your organizations safe.

IMPORTANT: UPGRADE TO LATEST SMA 100 SERIES FIRMWARE

SonicWall continues to **strongly recommend that all organizations using SMA 100 series products upgrade to the latest firmware released on Feb. 19**. The SMA 100 series is comprised of SMA 200, 210, 400, 410 physical appliances and the SMA 500v virtual appliance.

SonicWall also continues to **strongly recommend the enabling of multifactor authentication (MFA) on ALL products**, whether from SonicWall or from other vendors. If you have customers using SMA 100 series products, please proactively reach out to them to confirm they've upgraded or provide guidance on how to do so.

For details on how to upgrade firmware on SMA 100 series products or how to implement MFA, please visit the dedicated knowledgebase article: https://www.sonicwall.com/support/product-notification/210122173415410/