Zero-Day Exploits in SonicWall Email Security Lead to Enterprise Compromise

fireeye.com/blog/threat-research/2021/04/zero-day-exploits-in-sonicwall-email-security-lead-to-compromise.html

Threat Research

Josh Fleischer, Chris DiGiamo, Alex Pennino

Apr 20, 2021

12 mins read

Threat Research

Zero Day Threats

In March 2021, Mandiant Managed Defense identified three zero-day vulnerabilities in SonicWall's Email Security (ES) product that were being exploited in the wild. These vulnerabilities were executed in conjunction to obtain administrative access and code execution on a SonicWall ES device. The adversary leveraged these vulnerabilities, with intimate knowledge of the SonicWall application, to install a backdoor, access files and emails, and move laterally into the victim organization's network.

The vulnerabilities are being tracked in the following CVEs:

CVE-2021-20021	9.8	Unauthorized administrative account creation
CVE-2021-20022	7.2	Post-authentication arbitrary file upload
CVE-2021-20023	4.9	Post-authentication arbitrary file read

Mandiant has been coordinating with the SonicWall Product Security and Incident Response Team (PSIRT) for the responsible disclosure of this information. SonicWall advises all customers and partners to upgrade to the 10.0.9.6173 Hotfix for Windows users, and the 10.0.9.6177 Hotfix for hardware and ESXi virtual appliance users. SonicWall Hosted Email Security product was automatically updated for all customers and no additional action is required for patching purposes. The hotfixes will also be superseded by the upcoming SonicWall ES 10.0.10 release.

More information can be found by visiting the KB article published by SonicWall.

All patches, upgrades, and hotfixes are available to download on the MySonicWall site.

Overview

Figure 1: SonicWall Email Security ecosystem overview (via SonicWall)

SonicWall Email Security (ES) is an email security solution that "provides comprehensive inbound and outbound protection, and defends against advanced email-borne threats such as ransomware, zero-day threats, spear phishing and business email compromise (BEC)." The solution can be deployed as a physical appliance, virtual appliance, software installation, or a hosted SaaS solution.

Figure 2: Sample SonicWall Email Security login page

Like many appliances, the solution provides a rich, web-accessible administrative interface that serves as the main avenue for product configuration. Depending on the customer's deployment method, this software is potentially capable of running under Windows or Unix because it heavily leverages OS-independent Apache Tomcat and Java. While the solution doesn't require that this interface be exposed to the internet, internet-wide scanning shows approximately 700 publicly reachable interfaces.

Investigation

In March 2021, Mandiant Managed Defense identified post-exploitation web shell activity on an internet-accessible system within a customer's environment. Managed Defense isolated the system and collected evidence to determine how the system was compromised.

The system was quickly identified as a SonicWall Email Security (ES) application running on a standard Windows Server 2012 installation. The adversary-installed web shell was being served through the HTTPS-enabled Apache Tomcat web server bundled with SonicWall ES. Due to the web shell being served in the application's bundled web server, we immediately suspected the compromise was associated with the SonicWall ES application itself.

When we contacted the customer, we learned that the installation of SonicWall ES was the latest version available for download (10.0.9) and that there was no publicly available information pertaining to vulnerabilities or in-the-wild exploitation. To determine if a potential application-level vulnerability was exploited to install the web shell, Mandiant collected endpoint telemetry data.

We soon identified post-exploitation activity aimed at destroying evidence on the system, executed in the context of the web shell. The adversary executed the following command, shortly after installing the web shell:

```
cmd.exe /c "echo "" > "C:/Program Files (x86)/SonicWallES/logs/webUI/webui.json
```

Figure 3: The Adversary clearing existing entries in the current "webui.json" log

This command deleted the most recent application-level log entries recorded by the SonicWall ES web application. While clearing log files is a standard anti-forensics technique, understanding the location of internal log files generated by applications is usually overlooked by most spray-and-pray attackers. This added fuel to our suspicion that we were dealing with an adversary who had intimate knowledge of how the SonicWall ES application worked.

Fortunately for us, additional log files and a previously created virtual server snapshot provided enough evidence to track down the vulnerabilities and the adversary's activities on the host.

Vulnerabilities

CVE-2021-20021

Unauthenticated administrative access through improperly secured API endpoint

The SonicWall Email Security application contains an authenticated control panel to provide administration capabilities. One feature available allows application administrators to authorize an additional administrator account from a separate Microsoft Active Directory Organization Unit (AD OU).

```
https://<SonicWall ES host>/createou?data=<XML HERE>
```

Figure 4: A redacted example of the vulnerable endpoint associated with arbitrary user creation

Requests to this form, however, were not verified to require previous authentication to the appliance.

Due to this vulnerability, an adversary with a well-crafted XML document could either GET or POST their document to the application and create a “role.ouadmin” account (Figure 4). This account could then be used to authenticate to the application as an administrator.

CVE-2021-20022

Arbitrary file upload through post-authenticated “branding” feature

Like many enterprise products with a web-based user interface, SonicWall Email Security includes a feature known as "branding" which gives administrators the ability to customize and add certain assets to the interface, such as company logos. These branding assets are managed via packages, and new packages can be created by uploading ZIP archives containing custom text, image files, and layout settings. A lack of file validation can enable an adversary to upload arbitrary files, including executable code, such as web shells.

Once uploaded, these branding package ZIP archives are normally expanded and saved to the <SonicWall ES install path>\data\branding directory. However, an adversary could place malicious files in arbitrary locations, such as a web accessible Apache Tomcat directory, by crafting a ZIP archive containing a file within a sequence of directory traversal notations such as in Figure 5.

Figure 5: Example ZIP archive containing a Zip Slip web shell

It is important to note that the lack of validation which enables Zip Slip attacks is not unique to SonicWall Email Security. As detailed in Snyk's research on the topic, they exist within the many code libraries from which applications have been built.

CVE-2021-20023

Directory-traversal leads to arbitrary file read in post-authenticated "branding" feature

Mandiant confirmed another post-authentication vulnerability in the administrative panel's built-in "branding" feature which allowed an adversary to retrieve arbitrary files from the host by sending crafted HTTP GET requests to a particular resource. Figure 6 demonstrates the formatting of such request.

```
https://<SonicWall ES host>/dload_apps?action=<any value>&path=..%2F..%2F..%2F..%2F..%2Fwindows%2Fsystem32%2Fcalc.exe&id=update
```

Figure 6: An example web request which results in downloading the Windows calculator

While the working directory of this branding feature is <SonicWall ES install path>\data\updates, a directory-traversal vulnerability allows an adversary to access files located outside of this directory. As the Apache Tomcat webserver handling this request is operating as the NT AUTHORITY\SYSTEM account, any file on the operating system can be accessed.

Combinations of all three exploits were leveraged interchangeably by the adversary to perform the following actions:

1. Creation of a new Administrator account on the SonicWall ES device
2. Exposure of the hashed passwords for existing, locally configured Administrative accounts
3. The creation of a web shell in an arbitrary directory
4. Real-time debugging of exploitation success and failure

Post-Exploitation

Upon obtaining administrative access to the appliance through CVE-2021-20021, an adversary sent crafted HTTP requests to the resource /dload_apps, a component of the application's "branding" feature, exploiting CVE-2021-20023. These requests leveraged directory traversal attacks, enabling access to two sensitive XML configuration files located at <SonicWall ES install path>\data\multi_accounts.xml and <SonicWall ES install path>\data\multi_ldap.xml, respectively (Figure 7).

```
GET /dload_apps?action=REDACTED&path=..%2Fmulti_accounts.xml&id=update

GET /dload_apps?action=REDACTED&path=..%2Fmulti_ldap.xml&id=update
```

Figure 7: HTTP GET requests exploiting CVE-2021-20023

These files contained details about existing accounts as well as Active Directory credentials used by the application.

Next, the adversary uploaded a ZIP archive containing the BEHINDER JSP web shell from the administrative panel's "branding" page. The crafted ZIP archive used a Zip Slip attack to exploit CVE-2021-20022, which caused the web shell to be written to the web-accessible Apache Tomcat directory <SonicWall ES install path>\Apache Software Foundation\Tomcat 9.0\webapps\SearchEngineRMIService\.

BEHINDER is a publicly available, multi-platform web shell that accepts encrypted command and control (C2) communications. In principle, BEHINDER operates similarly to CHINA CHOPPER, a popular web shell that has been previously detailed by FireEye. Like CHINA CHOPPER, an adversary operates a client-side application to pass commands to the web shell within the body of HTTP requests. As the core functionality of the backdoor is contained within the client-side application, BEHINDER—much like CHINA CHOPPER—has the added benefit of being small, with the variant observed in this investigation weighing in at less than 1 kilobyte (Figure 8).

Figure 8: The BEHINDER web shell observed by Mandiant, which executes AES encrypted and base64 encoded commands

With the addition of a web shell to the server, the adversary had unrestricted access to the command prompt, with the inherited permissions of the NT AUTHORITY\SYSTEM account.

After clearing the SonicWall application “webui.json” log file, the adversary escalated their attack to credential harvesting in preparation of moving laterally into the victim's network. The adversary relied on “living off the land” techniques rather than bringing their own tools into the environment, which often has the benefit of potentially avoiding detections from a security product.

We observed the adversary executing the reg save command to dump the HKLM\SAM, HKLM\SYSTEM, and HKLM\SECURITY registry hives, which contain vital information in recovering password hashes and LSA secrets. Additionally, the adversary obtained in-memory sensitive credentials through the use of built-in memory dumping techniques. The adversary was observed invoking the MiniDump export of the Windows DLL comsvcs.dll to dump both the process memory for lsass.exe and the running instance of Apache Tomcat as seen in Figure 9.

```
rundll32.exe C:\windows\system32\comsvcs.dll, MiniDump <lsass PID>
c:\windows\temp\TS_LAS.dmp full

rundll32.exe C:\windows\system32\comsvcs.dll MiniDump <Tomcat PID>
C:\windows\temp\TS_FF9DG.dmp full
```

Figure 9: The adversary acquiring process memory for lsass.exe (MITRE ATT&CK T1003.001) and Apache Tomcat

Mandiant typically observes adversaries employing short and easy-to-type filenames during their operations, simply for efficiency. As such, the aforementioned filenames initially stood out as being peculiar, as a mix of case and symbols would require more effort to type than is often necessary. While this could always be indicative of a tool being used, the slight variations between the two commands—the absence of a comma before the DLL export and the uppercase C:\ drive in the second—suggest that they were manually typed. Considering that the C:\Windows\Temp\ directory on a Windows host also normally contains numerous similarly named temporary files, the adversary was likely taking extra care to evade suspicion should the activity reach the screen of a security analyst.

Continuing their effort to live off the land as much as possible, the adversary located a copy of the archiving utility 7-Zip already present on the host and used it to compress a subdirectory of <SonicWall ES install path>\data\archive\. This directory contains daily archives of emails processed by SonicWall ES—again demonstrating the adversary’s familiarity with the application.

After a several-day lull in activity, the adversary returned to the host, presumably after working to recover passwords from the registry hives and process memory that was dumped earlier. At the time of activity, the victim organization was using the same local Administrator

password across multiple hosts in their domain, which provided the adversary an easy opportunity to move laterally under the context of this account—highlighting the value of randomizing passwords to built-in Windows accounts on each host within a domain.

We observed the adversary leveraging Impacket's publicly available WMIEXEC.PY tool to access several internal hosts, which enabled remote command execution over Microsoft's DCOM protocol via Windows Management Instrumentation (WMI). The adversary managed to briefly perform internal reconnaissance activity prior to being isolated and removed from the environment.

Attribution

Mandiant currently tracks this activity as UNC2682. Ultimately, Mandiant prevented UNC2682 from completing their mission so their objectives of the attack currently remain unknown.

Each investigation conducted by Mandiant includes analysts from our Advanced Practices team who work to correlate activity observed in the thousands of investigations that Mandiant responds to. At times, we do not have the data available to directly attribute intrusion activity to a previously known group. In these cases, we create a new UNC group to track the activity that we observed. An UNC group is a cluster of related cyber intrusion activity, which includes observable artifacts such as adversary infrastructure, tools, and tradecraft, that we are not yet ready to give a classification such as APT or FIN.

For more details on how Mandiant uses UNC groups, see our blog post: DebUNCing Attribution: How Mandiant Tracks Uncategorized Threat Actors.

Investigation & Monitoring Tips

Mandiant recommends monitoring of the following endpoint telemetry indicators for potential evidence of compromise:

- Child processes of the web server process "tomcat" on SonicWall Email Security appliances, particularly cmd.exe
- The creation or existence of web shells on a server hosting SonicWall Email Security

In addition to standard indicators, Mandiant recommends reviewing SonicWall-related internal configuration files and logs for evidence of previous adversary activity.

Evidence of malicious web requests and their values may be identifiable in the following log files:

1. The Apache Tomcat logs:
   C:\Program Files\SonicWallES\Apache Software Foundation\Tomcat 9.0\logs
2. The SonicWall application logs:
   C:\Program Files\SonicWallES\logs\webUI\webui.json

Evidence of unauthorized modifications to SonicWall configuration settings can be confirmed in the following files:

1. The administration user account file:
   C:\Program Files\SonicWallES\data\multi_accounts.xml
2. Additional user account files that may have been created in the following directories:
   - C:\Program Files\SonicWallES\data\perhost
   - C:\Program Files\SonicWallES\data\perldap
   - C:\Program Files\SonicWallES\data\perou
3. Branding related zip files in any of the subdirectories of the following directory:
   C:\Program Files\SonicWallES\data\branding

Detecting the Techniques

FireEye detects this activity across our platforms. The following contains specific detection names that provide an indicator of SonicWall ES exploitation or post-exploitation activities associated with this adversary.

Product	Signature
FireEye Endpoint Security	• RUNDLL32.EXE COMSVCS.DLL PROCESS MINIDUMP (METHODOLOGY) • SUSPICIOUS REGISTRY EXPORTS (METHODOLOGY) • WEB SERVER ECHO REDIRECT (METHODOLOGY) • WEB SERVER CMD.EXE TYPE RECON (METHODOLOGY)
FireEye Network Security FireEye Email Security FireEye Detection On Demand FireEye Malware File Scanning FireEye Malware File Storage Scanning	• FE_PUP_Exploit_Linux_ZipSlip_1 • FE_Exploit_Win_ZipSlip_1 • FE_Trojan_ZIP_Generic_1 • FE_Webshell_JSP_BEHINDER_1 • FEC_Webshell_JSP_BEHINDER_1 • Webshell.JSP.BEHINDER • Webshell.JSP.BEHINDER.MVX
FireEye Helix	• METHODOLOGY - LFI [Null-Byte URI] • WMIEXEC UTILITY [Args] • WINDOWS METHODOLOGY [Unusual Web Server Child Process]

Additionally, SonicWall has deployed Intrusion Prevention System (IPS) signatures to SonicWall firewalls to help detect and block attacks that attempt to leverage the aforementioned vulnerabilities. The following signatures have already been applied to SonicWall firewalls with active security subscriptions:

- **IPS Signature**: 15520 WEB-ATTACKS SonicWall Email Security (CVE-2021-20022 Vulnerability)
- **IPS Signature**: 1067 WEB-ATTACKS Web Application Directory Traversal Attack 7
- **IPS Signature**: 15509 WEB-ATTACKS Web Application Directory Traversal Attack 7 - c2

Mandiant Security Validation Actions

Organizations can validate their security controls using the following actions with Mandiant Security Validation.

VID	Name
A101-563	Malicious File Transfer - BEHINDER, Download, Variant #1
A101-566	Web Shell Activity - BEHINDER, Basic Shell Interaction
A101-564	Malicious File Transfer - Zip Slip, Download, EICAR Variant
A101-565	Phishing Email - Malicious Attachment, Zip Slip, Generic Themed Lure

Vulnerability Disclosure

Mandiant disclosed the vulnerabilities CVE-2021-20021 and CVE-2021-20022 to SonicWall Product Security Incident Response Team (PSIRT) on March 26, 2021. The vulnerabilities were acknowledged and validated on March 29, 2021 and a hotfix became available on April 9, 2021. The patch was communicated to impacted SonicWall customers and partners on April 9, 2021.

Mandiant disclosed the vulnerability CVE-2021-20023 to SonicWall PSIRT on April 6, 2021. The vulnerability was acknowledged and validated on April 9, 2021 and a patch became available April 19.
To mitigate the three CVEs, Mandiant and SonicWall recommend upgrading Email Security to version 10.0.9.6173 (Windows) or 10.0.9.6177 (Hardware & ESXi Virtual Appliances). Organizations using SonicWall Hosted Email Security (HES) products were automatically updated and no action is required for those customers.

Acknowledgements

SonicWall PSIRT, Charles Carmakal, Ben Fedore, Geoff Ackerman and Andrew Thompson.