Health Sector Cybersecurity Coordination Center (HC3)
Sector Alert
April 22, 2021 TLP: White Report: 202104221600

SonicWall Zero-Day Vulnerabilities

Executive Summary

A recent security report identified 3 zero-day exploits for SonicWall Email Security (ES). Two of the three vulnerabilities were classified as High and Critical and can potentially allow for Threat Actors to extract sensitive information or compromise the device to use for their purposes. HC3 recommends all healthcare organizations immediately upgrade to the respective SonicWall ES versions. Patches are currently available for mitigation.

Report

In March 2021, security researchers identified suspicious web shell activity on a system within a customer's environment. The system was isolated to determine how it was compromised. During the investigation the system was identified as a SonicWall ES application on a standard Windows Server 2012 installation.

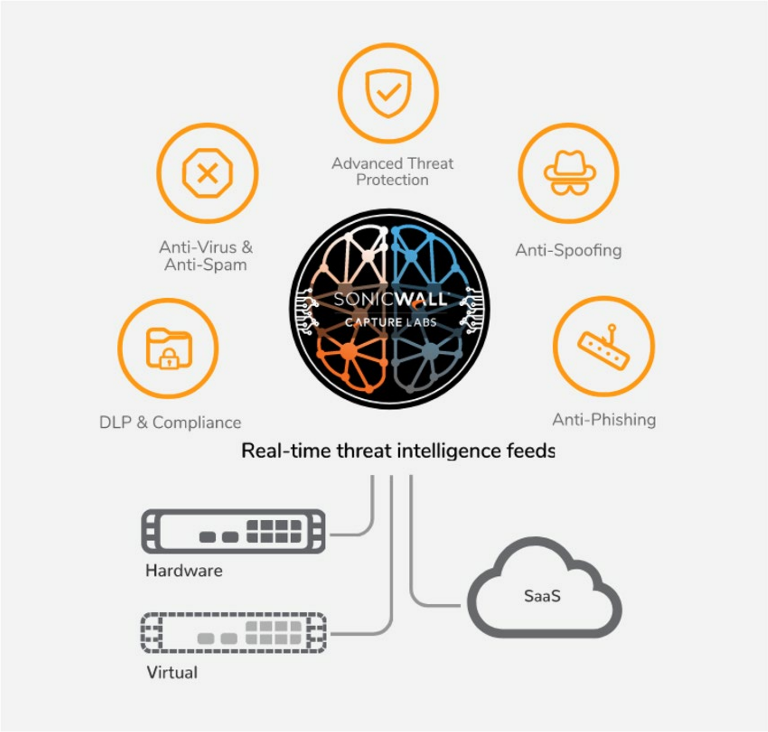
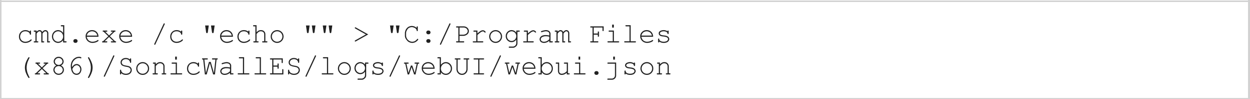


Figure 1: SonicWall Email Security ecosystem overview (via SonicWall)

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. The solution can be deployed as a physical appliance, virtual appliance, software installation, or a hosted SaaS solution.

The investigation noted that a malicious actor was executing the following command, shortly after installing the web shell:



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

Figure 2: The Adversary clearing existing entries in the current "webui.json" log

The intent of this command was to delete recent application-level log entries recorded by the SonicWall ES web application. The researchers also noted that the threat actor involved leveraged all three vulnerabilities and had extensive knowledge of the SonicWall application functions. The Threat Actor installed a backdoor, created an admin account, and accessed files and emails. More detailed analysis can be found via a FIREEYE report.

On April 20, 2021, SonicWall released a security advisory confirming 3 zero-day vulnerabilities affecting SonicWall ES. SonicWall researchers confirmed that "In at least one known case, these vulnerabilities have been observed to be exploited in the wild."

Analysis:

Recent targeting of security and discovery appliances has increased, creating a gateway for adversaries to collect and exploit connected hosts. The investigation revealed publicly available tools being used to access several internal hosts. This enabled remote command execution over the Windows Management Instrumentation (WMI) protocol DCOM. WMI can allow threat actors to perform many tactical functions such as gathering information for discovery and remote execution of files as a part of lateral movement. Process monitoring is key to assist in capturing command-line arguments of “wmic” and detect commands that are used to perform remote behavior.

Patches, Mitigations & Workarounds:

Patches

Vulnerability	Example Exploit	Affected Products
CVE-2021-20021	A vulnerability in the SonicWall Email Security version 10.0.9.x allows an attacker to create an administrative account by sending a crafted HTTP request to the remote host.	SonicWall On-premise Email Security (ES) 10.0.9 and earlier versions, Hosted Email Security (HES) 10.0.9 and earlier versions
CVE-2021-20022	SonicWall Email Security version 10.0.9.x contains a vulnerability that allows a post-authenticated attacker to upload an arbitrary file to the remote host.	SonicWall On-premise Email Security (ES) 10.0.9 and earlier versions, Hosted Email Security (HES) 10.0.9 and earlier versions
CVE-2021-20023	SonicWall Email Security version 10.0.9.x contains a vulnerability that allows a post-authenticated attacker to read an arbitrary file on the remote host.	SonicWall On-premise Email Security (ES) 10.0.9 and earlier versions, Hosted Email Security (HES) 10.0.9 and earlier versions

*SonicWall Hosted Email Security (HES) was patched on April 19, 2021, and no action is required from organizations that are only using the hosted email security product.

Mitigations

HC3 recommends users and administrators using SonicWall ES hardware appliances, virtual appliances or software installation on Microsoft Windows Server to immediately upgrade to the respective SonicWall Email Security recommended versions. SonicWall released patches for CVE-2021-20021 and CVE-2021-20022 on April 9, 2021, and for CVE-2021-20023 on April 20, 2021. Step-by-step guidance on how to apply the updates can be reviewed via SonicWall security advisory.

Continued Monitoring

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:

- The Apache Tomcat logs:
  - C:\Program Files\SonicWallES\Apache Software Foundation\Tomcat 9.0\logs

- 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:

- The administration user account file:
  - C:\Program Files\SonicWallES\data\multi_accounts.xml

- 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

- Branding related zip files in any of the subdirectories of the following directory:
  - C:\Program Files\SonicWallES\data\branding

References

Security Notice: SonicWall Email Security Zero-Day Vulnerabilities
https://www.sonicwall.com/support/product-notification/security-notice-sonicwall-email-security-zero-day-vulnerabilities/210416112932360/

Zero-Day Exploits in SonicWall Email Security Lead to Enterprise Compromise
https://www.fireeye.com/blog/threat-research/2021/04/zero-day-exploits-in-sonicwall-email-security-lead-to-compromise.html

Threat Actors Exploiting 3 SonicWall Email Security Vulnerabilities
https://healthitsecurity.com/news/threat-actors-exploiting-3-sonicwall-email-security-vulnerabilities

Hackers go after SonicWall email appliances with three zero-days
https://therecord.media/hackers-go-after-sonicwall-email-appliances-with-three-zero-days/

Hackers found leveraging three SonicWall zero-day vulnerabilities
https://www.helpnetsecurity.com/2021/04/21/sonicwall-email-security-zero-day-vulnerabilities/

Zero-day vulnerabilities in SonicWall email security are being actively exploited
https://www.zdnet.com/article/zero-day-vulnerabilities-in-sonicwall-email-security-are-being-exploited-in-

the-wild/

SonicWall Releases Patches for Email Security Products
https://us-cert.cisa.gov/ncas/current-activity/2021/04/21/sonicwall-releases-patches-email-security-products

CVE-2021-20021
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20021

SonicWall Security Advisory SNWLID-2021-0007
https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0007

CVE-2021-20022
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20022

SonicWall Security Advisory SNWLID-2021-0008
https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0008

CVE-2021-20023
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-20023

SonicWall Security Advisory SNWLID-2021-0010
https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0010