# HelloKitty ransomware is targeting vulnerable SonicWall devices

**bleepingcomputer.com**/news/security/hellokitty-ransomware-is-targeting-vulnerable-sonicwall-devices/

Sergiu Gatlan

By
Sergiu Gatlan

- July 17, 2021
- 11:44 AM
- 0

CISA warns of threat actors targeting "a known, previously patched, vulnerability" found in SonicWall Secure Mobile Access (SMA) 100 series and Secure Remote Access (SRA) products with end-of-life firmware.

As the US federal agency also adds, the attackers can exploit this security vulnerability as part of a targeted ransomware attack.

This alert comes after SonicWall issued an "urgent security notice" and sent emails to warn customers of the "imminent risk of a targeted ransomware attack."

Even though the company said the risk of ransomware attacks is imminent, Coveware CEO Bill Siegel confirmed CISA's warning saying that the campaign is ongoing.

CISA urges users and administrators to review the SonicWall security notice and upgrade their devices to the latest firmware or immediately disconnect all end-of-life appliances.

> Upgrade to the newest SonicWall firmware and disconnect EOL SonicWall appliances ASAP. Failing to follow SonicWall guidance may lead to targeted ransomware attacks. Read more at https://t.co/ji96tw5Md4 #Cybersecurity #InfoSec #Ransomware
>
> — US-CERT (@USCERT_gov) July 15, 2021

## HelloKitty ransomware: one of the groups behind these attacks

While CISA and SonicWall did not reveal the identity of the threat attackers behind these attacks, BleepingComputer was told by a source in the cybersecurity industry that HelloKitty has been exploiting the vulnerability for the past few weeks.

Cybersecurity firm CrowdStrike also confirmed to BleepingComputer that the ongoing attacks are attributed to multiple threat actors, including HelloKitty.

HelloKity is a human-operated ransomware operation active since November 2020, mostly known for encrypting the systems of CD Projekt Red and claiming to have stolen Cyberpunk 2077, Witcher 3, Gwent, and other games' source code.

Even though the bug abused to compromise unpatched and EOL SMA and SRA products was not disclosed in CISA's warning or SonicWall's notice, CrowdStrike security researcher Heather Smith told BleepingComputer yesterday that the targeted vulnerability is tracked as CVE-2019-7481.

"This exploitation targets a long-known vulnerability that was patched in newer versions of firmware released in early 2021," SonicWall said in an emailed statement.

However, CrowdStrike's Heather Smith and Hanno Heinrichs said in a report published last month that "CrowdStrike Services incident response teams identified eCrime actors leveraging an older SonicWall VPN vulnerability, CVE-2019-7481, that affects Secure Remote Access (SRA) 4600 devices."

SonicWall credited the two security researchers with reporting the actively exploited security flaw in a security advisory issued yesterday.

According to a Coveware report, Babuk ransomware is also targeting SonicWall VPNs likely vulnerable to CVE-2020-5135 exploits. This vulnerability was patched in October 2020 but it is still "heavily abused by ransomware groups today" per Coveware.

## Ransomware vs. SonicWall devices

A threat group tracked by Mandiant as UNC2447 has also exploited the CVE-2021-20016 zero-day bug in SonicWall SMA 100 Series VPN appliances to deploy a new ransomware strain known as FiveHands (a DeathRansom variant just as HelloKitty).

Their attacks targeted multiple North American and European targets before SonicWall released patches in late February 2021.

The same zero-day was also abused in January in attacks targeting SonicWall's internal systems and later indiscriminately exploited in the wild.

Mandiant threat analysts discovered three other zero-day vulnerabilities in SonicWall's on-premises and hosted Email Security (ES) products in March.

These three zero-days were also actively exploited by a group Mandiant tracks as UNC2682 to backdoor systems using BEHINDER web shells, allowing them to move laterally through victims' networks and access emails and files.

"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 Mandiant researchers said at the time.

## Related Articles:

QNAP alerts NAS customers of new DeadBolt ransomware attacks

SonicWall ‘strongly urges’ admins to patch SSLVPN SMA1000 bugs

QNAP warns of ransomware targeting Internet-exposed NAS devices

BlackCat/ALPHV ransomware asks $5 million to unlock Austrian state

Intuit warns of QuickBooks phishing threatening to suspend accounts