SonicWall fixes critical bug allowing SMA 100 device takeover

By **Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)** September 24, 2021 02:19 AM **0**

SonicWall has patched a critical security flaw impacting several Secure Mobile Access (SMA) 100 series products that can let unauthenticated attackers remotely gain admin access on targeted devices.

The SMA 100 series appliances vulnerable to attacks targeting the improper access control vulnerability tracked as CVE-2021-20034 (https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0021) includes SMA 200, 210, 400, 410, and 500v.

There are no temporary mitigations to remove the attack vector, and SonicWall *strongly urges* impacted customers to deploy security updates that address the flaw *as soon as possible*.

No in the wild exploitation

Successful exploitation can let attackers delete arbitrary files from unpatched SMA 100 secure access gateways to reboot to factory default settings and potentially gain administrator access to the device.

"The vulnerability is due to an improper limitation of a file path to a restricted directory potentially leading to arbitrary file deletion as nobody," the company said (https://www.sonicwall.com/support/product-notification/security-notice-critical-arbitrary-file-delete-vulnerability-in-sonicwall-sma-100-series-appliances/210819124854603/).

SonicWall asked organizations using SMA 100 series appliances to immediately log in to MySonicWall.com to upgrade the appliances to the patched firmware versions outlined in the table embedded below.

The company found no evidence that this critical pre-auth vulnerability is currently being exploited in the wild.

Product	Platform	Impacted Version	Fixed Version
SMA 100 Series	• SMA 200 • SMA 210 • SMA 400 • SMA 410	10.2.1.0-17sv and earlier	10.2.1.1-19sv and higher
		10.2.0.7-34sv and earlier	10.2.0.8-37sv and higher

	• SMA 500v (ESX, KVM, AWS, Azure)	9.0.0.10-28sv and earlier	9.0.0.11-31sv and higher

Ransomware targeting

SonicWall SMA 100 series appliances have been targeted by ransomware gangs multiple times since the start of 2021, with the end goal of moving laterally into the target organization's network

For instance, a threat group Mandiant tracks as UNC2447 exploited the CVE-2021-20016 (https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001) zero-day bug in SonicWall SMA 100 appliances to deploy a new ransomware strain known as FiveHands (https://www.bleepingcomputer.com/news/security/new-ransomware-group-uses-sonicwall-zero-day-to-breach-networks/) (a DeathRansom variant just as HelloKitty).

Their attacks targeted multiple North American and European organizations before security updates were released in late February 2021 (https://www.bleepingcomputer.com/news/security/sonicwall-firewall-maker-hacked-using-zero-day-in-its-vpn-device/). The same flaw was also exploited in January in attacks targeting SonicWall's internal systems (https://www.bleepingcomputer.com/news/security/sonicwall-firewall-maker-hacked-using-zero-day-in-its-vpn-device/) and later indiscriminately abused in the wild (https://www.bleepingcomputer.com/news/security/sonicwall-sma-100-zero-day-exploit-actively-used-in-the-wild/).

Two months ago, in July, SonicWall warned of an increased risk of ransomware attacks (https://www.bleepingcomputer.com/news/security/sonicwall-warns-of-critical-ransomware-risk-to-eol-sma-100-vpn-appliances/) targeting unpatched end-of-life (EoL) SMA 100 series and Secure Remote Access (SRA) products.

CrowdStrike and Coveware security researchers added to SonicWall's warning saying that the ransomware campaign was ongoing. CISA confirmed the researchers' findings three days later

(https://www.bleepingcomputer.com/news/security/hellokitty-ransomware-is-targeting-vulnerable-sonicwall-devices/), warning that threat actors were targeting a previously patched SonicWall vulnerability

BleepingComputer also reported at the time that HelloKitty ransomware had been exploiting the vulnerability (tracked as CVE-2019-7481) for a few weeks before SonicWall's 'urgent security notice' was issued.

SonicWall recently revealed (https://blog.sonicwall.com/en-us/2021/08/sonicwall-celebrating-three-decades-of-putting-customers-first/) that its products are used by more than 500,000 business customers in over 215 countries and territories worldwide. Many of them are deployed on the networks of the world's largest organizations, enterprises, and government agencies.

Related Articles:

New Windows security updates break network printing (https://www.bleepingcomputer.com/news/security/new-windows-security-updates-break-network-printing/)

Cisco: Firewall manager RCE bug is a zero-day, patch incoming (https://www.bleepingcomputer.com/news/security/cisco-firewall-manager-rce-bug-is-a-zero-day-patch-incoming/)

Bot protection now generally available in Azure Web Application Firewall (https://www.bleepingcomputer.com/news/security/bot-protection-now-generally-available-in-azure-web-application-firewall/)

Hackers are scanning for VMware CVE-2021-22005 targets, patch now! (https://www.bleepingcomputer.com/news/security/hackers-are-scanning-for-vmware-cve-2021-22005-targets-patch-now/)

New macOS zero-day bug lets attackers run commands remotely (https://www.bleepingcomputer.com/news/apple/new-macos-zero-day-bug-lets-attackers-run-commands-remotely/)

FIREWALL (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/FIREWALL/)

SONICWALL (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/SONICWALL/)

VULNERABILITY (HTTPS://WWW.BLEEPINGCOMPUTER.COM/TAG/VULNERABILITY/)