Google finds custom backdoor being installed on SonicWall network devices

Researchers from the Google Threat Intelligence Group said that hackers are compromising SonicWall Secure Mobile Access (SMA) appliances, which sit at the edge of enterprise networks and manage and secure access by mobile devices.

The targeted devices are end of life, meaning they no longer receive regular updates for stability and security. Despite the status, many organizations continue to rely on them. That has left them prime targets by UNC6148, the name Google has given to the unknown hacking group.

“GTIG recommends that all organizations with SMA appliances perform analysis to determine if they have been compromised,” a report published Wednesday said, using the abbreviation for Google Threat Intelligence Group. “Organizations should acquire disk images for forensic analysis to avoid interference from the rootkit anti-forensic capabilities. Organizations may need to engage with SonicWall to capture disk images from physical appliances.”

Lacking specifics

Many key details remain unknown. For one thing, the attacks are exploiting leaked local administrator credentials on the targeted devices, and so far, no one knows how the credentials were obtained. It’s also not known what vulnerabilities UNC6148 is exploiting. It’s also unclear precisely what the attackers are doing after they take control of a device.

The lack of details is largely the result of the functioning on Overstep, the name of custom backdoor malware UNC6148 is installing after initial compromise of the devices. Overstep allows the attackers to selectively remove log entries, a technique that is hindering forensic investigation. Wednesday's report also posits that the attackers may be armed with a zero-day exploit, meaning it targets a vulnerability that's currently publicly unknown. Possible vulnerabilities UNC6148 may be exploiting include:

- CVE-2021-20038: An unauthenticated remote code execution made possible by a memory corruption vulnerability.
- CVE-2024-38475: An unauthenticated path traversal vulnerability in Apache HTTP Server, which is present in the SMA 100. It can be exploited to extract two separate SQLite databases that store user account credentials, session tokens, and seed values for generating one-time passwords.
- CVE-2021-20035: An authenticated remote code execution vulnerability. Security firm Arctic Wolf and SonicWall reported in April that this vulnerability was under active exploitation.
- CVE-2021-20039: An authenticated remote code execution vulnerability. There have been reports that this vulnerability was under active exploitation to install ransomware in 2024.
- CVE-2025-32819: An authenticated file deletion vulnerability that can be exploited to cause a targeted device to revert the built-in administrator credentials to a password so that attackers can gain administrator access.

https://arstechnica.com/security/2025/07/google-finds-custom-backdoor-being-installed-on-sonicwall-network-devices/