SonicWall SSL VPN Attacks Escalate, Bypassing MFA

Data: 2025-09-29 10:30:00

Autor: Inteligência Against Invaders

Security experts have warned of a surge in malicious activity from Akira ransomware actors targeted

at victims running SonicWall SSL VPN appliances.

The campaign appears to have begun back in late July, with initial reports suggesting a zero-day vulnerability may have been to blame.

Thesewere later dismissed, with legacy bug CVE-2024-40766 blamed for initial access.

A new report published on Friday by Arctic Wolf claimed that exploitation of this improper access control vulnerability supported credential harvesting. This subsequently enabled those devices to be targeted, even if they had been patched, it said.

“With dwell times measured in hours rather than days – among the shortest we’ve recorded for ransomware – the window for effective response against this threat is exceptionally narrow,” Arctic Wolf warned.

Read more on SonicWall VPN attacks:SonicWall Discloses Compromise of Cloud Backup Service

The report claimed that most attacks observed in this campaign contain similar elements:

- VPN client logins originating from hosting providers
- Internal network scanning
- Impacket SMB activity tied to discovery
- Active Directory discovery

OTP Bypass

Interestingly, the threat actors have also been able to compromise devices running one-time password (OTP) multi-factor authentication (MFA).

“In our investigation, we observed repeated malicious SSL VPN logins on accounts with OTP MFA enabled, ruling out scratch code usage in those cases. We also found no signs of malicious use of the compromised accounts prior to SSL VPN login, nor did we observe unauthorized OTP unbinding events or other malicious configuration changes in the five days leading up to the intrusions,” the report continued.

“Taken together, the evidence points to the use of valid credentials rather than modification of OTP configuration, though the exact method of authenticating against MFA-enabled accounts remains unclear.”

One possible explanation is that threat actors managed to obtain OTP seeds.

“Google Threat Intelligence Group recently uncovered a campaign affecting SonicWall SMA demonstrating that if OTP seeds are obtained by threat actors, they can be used to generate valid OTP tokens,” Arctic Wolf said.

There are also hints that adversaries used automated tooling to achieve initial access and lateral movement. Arctic Wolf said it recorded multiple login events in quick succession across a number of accounts, from the same VPN client IP address.

“Upon gaining SSL VPN access, threat actors wasted no time in attempting lateral movement through compromised environments, typically initiating internal scanning within five minutes of logging in,” it added.

Bring-Your-Own-Vulnerable-Driver (BYOVD) techniques were also used to evade detection by security tools.

“Early detection is critical in this campaign, and to that end we recommend monitoring for hosting-related ASNs in SonicWall SSL VPN logins,” Arctic Wolf concluded.

“Additionally, monitoring for SMB session setup requests consistent with Impacket provides an early kill chain detection for discovery activity related to this campaign.”

The security vendor[also advised](#) blocking logins from infrastructure linked to virtual private server(VPS) hosting providers and anonymization services, as well as restricting VPN logins from countries where the organization does not do business.