Akira ransomware breaching MFA-protected SonicWall VPN accounts

Data: 2025-09-28 19:50:28

Autor: Inteligência Against Invaders

Ongoing Akira ransomware attacks targeting SonicWall SSL VPN devices continue to evolve, with the threat actors found to be successfully authenticating despite OTP MFA being enabled on accounts. Researchers suspect this may through the use of previously stolen OTP seeds, though the exact method remains unconfirmed at this time.

In July, BleepingComputer reported that the Akira ransomware operation was exploiting SonicWall SSL VPN devices to breach corporate networks, leading researchers to suspect that a zero-day flaw was being exploited to compromise these devices.

However, SonicWall ultimately linked the attacks to an improper access control flaw tracked asCVE-2024-40766 that was disclosed in September 2024.

While the flaw was patched in August 2024, threat actors have continued to use credentials previously stolen from exploited devices, even after the security updates were applied.

After linking the attacks to credentials stolen using CVE-2024-40766, SonicWall urged administrators to reset all SSL VPN credentials and ensure that the latest SonicOS firmware was installed on their devices.

New research shows MFA bypassed

Cybersecurity firm Arctic Wolf now reports observing an ongoing campaign against SonicWall firewalls, where threat actors aresuccessfully logging into accounts even when one-time password (OTP) multi-factor authentication is enabled.

The report indicates that multiple OTP challenges were issued for account login attempts, followed by successful logins, suggesting that threat actors may have also compromised OTP seeds or discovered an alternative method to generate valid tokens.

[IMAGEM REMOVIDA]links the malicious logins observed in this campaign toCVE-2024-40766, an improper access control vulnerability identified a year ago," explains Arctic Wolf.

"From this perspective, credentials would have potentially been harvested from devices vulnerable to CVE-2024-40766 and later used by threat actors—even if those same devices were patched. Threat actors in the present campaign successfully authenticated against accounts with the one-time password (OTP) MFA feature enabled."

While the researchers say it's unclear how Akira affiliates are authenticating to MFA-protected accounts, a separate report from Google Threat Intelligence Group in July described similar abuse of SonicWall VPNs.

In that campaign, a financially motivated group tracked as UNC6148 deployed the OVERSTEP rootkit on SMA 100 series appliances by using what they believe are previously stolen OTP seeds, allowing access even after patches were applied.

Google believes that the threat actors were utilizing stolen one-time password seeds that were previously obtained in zero-day attacks, but is unsure which CVE was exploited.

"Google Threat Intelligence Group (GTIG) has identified an ongoing campaign by a suspected financially-motivated threat actor we track as UNC6148, targeting fully patchedend-of-life SonicWall Secure Mobile Access (SMA) 100 series appliances," warned Google.

"GTIG assesses with high confidence that UNC6148 is leveraging credentials and one-time password (OTP) seeds stolen during previous intrusions, allowing them to regain access even after organizations have applied security updates."

Once inside, Arctic Wolf reports that Akira moved very quickly, often scanning the internal network within 5 minutes. The researchers note that the threat actors also employed Impacket SMB session setup requests, RDP logins, and the enumeration of Active Directory objects using tools such as dsquery, SharpShares, and BloodHound.

A particular focus was on Veeam Backup & Replication servers, where a custom PowerShell script was deployed to extract and decrypt stored MSSQL and PostgreSQL credentials, including DPAPI secrets.

To evade security software, affiliates conducted a Bring-Your-Own-Vulnerable-Driver (BYOVD) attack by abusing Microsoft's legitimate consent.exe executable to sideload malicious DLLs that loaded vulnerable drivers (rwdrv.sys, churchill_driver.sys).

These drivers were used to disable endpoint protection processes, allowing the ransomware encryptors to run without being blocked.

The report stresses that some of these attacks impacted devices running SonicOS 7.3.0, which is the recommended release SonicWall urged admins to install to mitigate the credential attacks.

Admins are strongly urged to reset all VPN credentials on any device that previously utilized vulnerable firmware, as even if updated, attackers can continue to use stolen accounts to gain initial access to corporate networks.

[IMAGEM REMOVIDA]