

Forum:[Hack Forums](#)

Thread: [Akira Ransomware Group Utilizing SonicWall Devices for Initial Access](#)

MadScientist - September 14, 2025, 8:48 am

In August 2024, SonicWall published a security advisory for CVE SNWLID-2024-0015, which was related to improper access control vulnerability for SSLVPN affecting Gen5, Gen6, and Gen7 firewall appliances. This vulnerability allowed unauthorized access to SonicWall in specific conditions. This vulnerability has since been addressed and patches provided from SonicWall.

Last month, an Akira ransomware campaign kicked off targeting SonicWall devices. SonicWall followed up with a security advisory. Initially, this was believed to be a new emerging threat, but SonicWall has since disclosed that this is related to the August 2024 CVE (SNWLID-2024-0015), in which remediation steps were not successfully completed. Rapid7 responded by sending emergent threat communications to our customers alerting them to this threat and advising them to prioritize patching. Since that time, the Rapid7 Incident Response (IR) team has observed an uptick in intrusions involving SonicWall appliances.

Following its initial communication last month, SonicWall posted additional security guidance around the SSLVPN Default Users Group Security Risk. This is a security risk which, in certain configurations, can over provision access to SonicWall's SSLVPN services based on the Default LDAP group configurations. This can allow users who are not permitted to SSLVPN to successfully obtain access to the SSLVPN irrespective of Active Directory configurations.

Rapid7 has also observed threat actors accessing the Virtual Office Portal hosted by SonicWall appliances. The Virtual Office Portal can be used to initially set up MFA/TOTP configurations for SSLVPN users. The Virtual Office Portal in certain default configurations allows public access to the portal, which can allow threat actors to configure MFA/TOTP with valid accounts if there is a prior username and password credential exposure.

Evidence collected during Rapid7's investigations suggests that the Akira group is potentially utilizing a combination of all three of these security risks to gain unauthorized access and conduct ransomware operations.

Source -

<https://www.rapid7.com/blog/post/dr-akira-ransomware-group-utilizing-sonicwall-devices-for-initial-access/>

Lowkey - September 14, 2025, 8:50 am

Are you and Stanely the new HF bots?

This is bot behavior.

Bots.

MadScientist - September 14, 2025, 8:52 am

(Sep 14, 2025 08:50 AM)Lowkey Wrote: [CITE](#) Are you and Stanely the new HF bots?

This is bot behavior.

Bots.

Stanley needed some competition ? Haha just sharing some of the articles I was reading this morning and found interesting ?

Lowkey - *September 14, 2025, 8:53 am*

(Sep 14, 2025 08:52 AM)MadScientist Wrote: [\[CITE\]](#) Stanley needed some competition ? Haha just sharing some of the articles I was reading this morning and found interesting ?

Very cool. Carry on.