

THREAT BULLETINS

Akira Ransomware is Actively Targeting SonicWall SSL VPNs



TLP:WHITE

Aug 04, 2025

On August 1, 2025, SonicWall released a [report](#) claiming they have identified a significant increase in ransomware activity targeting SonicWall SSL VPNs for initial network access starting in late July 2025. The company claims evidence suggests these attacks might be leveraging a zero-day vulnerability. Cyber company Huntress has also allegedly [observed](#) threat actors trying to gain access to networks using SonicWall devices.

While SonicWall has not confirmed the existence of a zero-day vulnerability, this alert is shared for your situational awareness.

In this latest campaign, threat actors are authenticating using Virtual Private Server (VPS) hosting, in stark contrast to legitimate VPN traffic from broadband providers. This enables them to quickly transition from initial access to ransomware deployment.

The evidence that points to a zero-day vulnerability lies in the fact that even fully patched devices with multi-factor authentication (MFA) enabled are being compromised.

The most recent campaign, which began around July 15, is linked to the Akira ransomware group. Akira ransomware is a financially motivated threat actor that has targeted companies, including critical infrastructure entities globally, since 2023. They target Windows and VMware ESXi virtual machines with a Linux variant. They use phishing emails or vulnerability exploitation to gain a foothold in the victims' environment. Additional identified methods also include credential abuse and leveraging exposed RDP access. They also used a variety of other tools such as AdFind, Advanced IP Scanner, AnyDesk, Mimikatz, RClone, WinRAR, WinSCP, and PowerShell to conduct reconnaissance, credential theft, system manipulation, and remote access. These malicious actions, if successful, ultimately result in data theft and encryption, which is followed by double extortion. More information on the threat actor is available in CISA's report [#StopRansomware: Akira Ransomware](#).

Based on the observed tactics and the high likelihood of unpatched vulnerability, below are some actionable recommendations to help Health-ISAC members using SonicWall SSL VPN devices to protect their environment from the ongoing exploitation.

Recommendations

- **Disable the SonicWall SSL VPN service:** Given the strong evidence of a zero-day vulnerability, immediately disabling the SonicWall SSL VPN service is the most effective way to prevent initial access. This should remain in effect until a vendor-provided patch is available and successfully deployed.
- **Enforce and review strong access controls:** Actively block VPN authentication requests originating from known hosting-related Autonomous System Numbers (ASNs). While these networks are not inherently malicious, their use for VPN access is highly suspicious and indicative of attacker activity.
- **Enhance MFA across organizational accounts:** Ensure MFA is enforced for all remote access accounts. Additionally, regularly audit and remove unused or inactive local firewall user accounts, especially those with SSL VPN privileges, to reduce the attack surface.
- **Strengthen endpoint and network monitoring:** Enhance your visibility by deploying an Endpoint Detection and Response (EDR) solution. Log entries from unexpected sources,

particularly from VPS or cloud hosting providers, should be considered high-priority alerts for investigation.

- Prioritize patching management: Once SonicWall releases a patch, apply it immediately to mitigate the risk of exploitation.

Reference(s)

[arcticwolf](#), [cisa](#), [socradar](#), [linkedin](#)

Sources

<https://arcticwolf.com/resources/blog/arctic-wolf-observes-july-2025-uptick-in-akira-ransomware-activity-targeting-sonicwall-ssl-vpn/>

https://www.linkedin.com/posts/drayagha_sonicwall-exploitation-zero-day-activity-7357432800796364801-urh0/

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a>

<https://socradar.io/dark-web-profile-akira-ransomware/>



Incident Date

Aug 04, 2025 (UTC)

Alert ID 81378578

[View Alert](#)

Share Feedback

was this helpful?  | 

Tags SonicWall SSL VPN, Akira Ransomware

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.



For more updates and alerts, visit: <https://health-isac.cyware.com/webapp/>

If you are not supposed to receive this email,
please contact us at toc@h-isac.org.