AL2025_35 SonicWall Devices Exploited in Latest Akira Ransomware Campaign (August 8th, 2025)

Description

There has been a surge in Akira ransomware attacks targeting SonicWall firewall devices with SSL VPN enabled, initially suspected to be exploiting a previously undiscovered zero-day vulnerability. However, SonicWall has since clarified that this spike in activity is not linked to a new zero-day. Instead, there is strong evidence connecting the attacks to **CVE-2024-40766**, a high-severity (CVSS score: 9.3) improper access control vulnerability disclosed in August 2024. This flaw, affecting SonicOS management access, could allow unauthorized resource access and, under certain conditions, cause a firewall crash.

SonicWall further noted that many recent incidents involved organizations migrating from Gen 6 to Gen 7 firewalls without resetting local user passwords contrary to security recommendations for mitigating CVE-2024-40766. While the vulnerability has been patched, failure to follow migration best practices has left some devices exposed to credential-based attacks, password reuse, and brute-force attempts.

Attack Details

Arctic Wolf Labs observed multiple intrusions beginning on July 15, 2025, leveraging SonicWall SSL VPN access as the primary entry point. While brute-force, dictionary, and credential-stuffing attacks remain possible, the evidence now indicates exploitation of older vulnerabilities combined with weak password hygiene, rather than a zero-day. Once inside, attackers escalated privileges, stole credentials, disabled security tools, and deployed ransomware in patterns consistent with Akira's known tactics. Threat actors made use of Virtual Private Servers (VPS) to connect via VPN differentiating their traffic from legitimate broadband users and enhancing anonymity.

Cybersecurity vendors, including Huntress, continue to report active exploitation of SonicWall Gen 7 firewall appliances. As of August 6, 2025, at least 28 confirmed incidents have been recorded, with targeting linked to both Akira and Fog ransomware groups.

Indicators of Compromise (IoCs)

Administrators should look out for the following signs of compromise:

- Unusual or unauthorized access logs via SonicWall SSL VPN
- VPN authentication originating from VPS-hosting providers
- Sudden appearance of OVERSTEP rootkit malware on systems
- Suspicious administrative activity or unauthorized configuration changes
- Connection attempts using brute-force or credential-stuffing patterns

Remediation

Arctic Wolf and SonicWall recommend the following actions:

Immediate Actions:

1. Apply all security patches for SonicWall SMA 100 appliances and firewall devices, including fixes for **CVE-2024-40766**.
2. Temporarily disable SSL VPN services on Gen 7 devices until secure configuration and patching are confirmed.
3. Review VPN and system logs for unauthorized access.
4. Block VPN authentication attempts from VPS and hosting provider IP ranges.
5. Implement endpoint monitoring, enhanced logging, and multi-factor authentication (MFA).

Updated SonicWall Recommendations:

1. Upgrade firmware to **SonicOS version 7.3.0** for added brute-force and MFA protections.
2. Reset **all local user account passwords**, especially those migrated from Gen 6 to Gen 7.
3. Enable Botnet Protection and Geo-IP Filtering.
4. Enforce strong password policies and MFA on all accounts.
5. Remove unused or inactive accounts.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Gatlan, S. (2025, August 1). SonicWall firewall devices hit in surge of Akira ransomware attacks. BleepingComputer. https://www.bleepingcomputer.com/news/security/surge-of-akira-ransomware-attacks-hits-sonicwall-firewall-devices/
- Team, F. E. S. I. (2025, August 2). Akira ransomware targeting SonicWall VPN appliances. *Field Effect Security Intelligence Team*. https://fieldeffect.com/blog/akira-ransomware-targeting-sonicwall-vpn-appliances
- Lyons, J. (2025, August 4). SonicWall investigates "cyber incidents," including ransomware targeting suspected 0-day. *The Register*. https://www.theregister.com/2025/08/04/sonicwall_investigates_cyber_incidents/
- The Hacker News. (n.d.). *SonicWall confirms patched vulnerability behind recent VPN attacks, not a Zero-Day*. https://thehackernews.com/2025/08/sonicwall-confirms-patched.html?m=1