AL2025_43 Akira Ransomware Exploits SonicWall VPNs to Bypass Multi-Factor Authentication (September 29th , 2025)

Description

Security researchers have observed the Akira ransomware group bypassing multi-factor authentication (MFA) protections on **SonicWall SSL VPN appliances**. Attackers are leveraging credentials and one-time password (OTP) seeds stolen during earlier SonicWall zero-day exploits, allowing them to log in even on patched and MFA-protected devices. Once inside, Akira affiliates move quickly to compromise networks, steal data, and deploy ransomware.

Attack Details

- Attackers target SonicWall VPNs previously affected by CVE-2024-40766.
- OTP MFA codes are bypassed, likely using stolen or compromised OTP seeds.
- Arctic Wolf observed multiple OTP challenges during logins, followed by successful authentications.
- Once authenticated, attackers conduct reconnaissance with tools such as **dsquery**, **SharpShares**, and **BloodHound**.
- Backups are targeted: PowerShell scripts extract credentials from **Veeam Backup & Replication** systems.
- Akira affiliates use Bring-Your-Own-Vulnerable-Driver (BYOVD) techniques to disable security software.

Remediation

- **Update and Patch**: Ensure SonicWall appliances are updated to the latest firmware version.

- **Reset VPN Credentials**: Change all VPN account passwords and revoke previously issued OTP seeds.

- **Enable Advanced MFA**: Consider hardware tokens or app-based authenticators with anti-cloning protections.

- **Restrict VPN Exposure**: Limit VPN access to trusted IP ranges or enforce geolocation restrictions.

- **Monitor Logs**: Review VPN and authentication logs for repeated OTP prompts or suspicious login attempts.

- **Secure Backups**: Protect backup servers with strong credentials and isolate them from production networks.

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

References

- Abrams, L. (2025, September 27). Akira ransomware breaching MFA-protected SonicWall VPN accounts. BleepingComputer. Retrieved from https://www.bleepingcomputer.com/news/security/akira-ransomware-breaching-mfa-protected-sonicwall-vpn-accounts/

- CybersecurityNews. (2025, September 27). SonicWall firewalls targeted by Akira ransomware operators. CybersecurityNews. Retrieved from https://cybersecuritynews.com/sonicwall-firewalls-akira-ransomware/