U UNISPHERE SOLUTIONS

✉ info@unisphere.co.nz
🌐 www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00094

SONICWALL VPN VULNERABILITY EXPLOITED

DATE ISSUED: 26th January 2021

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	[✓ MEDIUM]	EASY

OVERVIEW

Attackers have exploited SonicWall VPN vulnerability in the Secure Mobile Access (SMA) 100 series appliances in a zero-day attack.

BREAKDOWN

At this stage, SonicWall has identified that this new vulnerability will only affect the SMA 100 series and no other products. The NetExtender VPN client has been ruled out through investigation as being vulnerable and remains safe to use with SonicWall products. The zero-day attack seems likely to have been conducted by sophisticated attackers in a coordinated effort to target internal systems. The root cause is still under investigation.

REMEDIATION STEPS

- Lock down VPN access to affected SMA appliances through IP allowlist
- Configure and enforce MFA on all VPN access as well as any other connection methods to SonicWall VPN
- If you have logging enabled or other network monitoring, check and remain vigilant for anomalous activity
- Monitor security advisories from SonicWall using the reference below
- Contact your reseller or CERT NZ for further information regarding your concerns

REFERENCES & RESOURCES

CERT NZ	https://www.cert.govt.nz/it-specialists/advisories/vulnerability-in-sonicwall-vpn-products-exploited/
SonicWall	https://www.sonicwall.com/support/product-notification/urgent-security-notice-probable-sma-100-series-vulnerability-updated-jan-25-2021/210122173415410/ https://psirt.global.sonicwall.com/vuln-list
SC Magazine	https://www.scmagazine.com/home/security-news/vulnerabilities/sonicwall-network-attacked-via-zero-days-in-its-vpn-and-secure-access-solutions/