مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

SonicWall Urges Credential Reset Following Configuration Backup Leak

Tracking #:432317729

Date:19-09-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed SonicWall has issued a critical advisory after firewall configuration backups were leaked, potentially exposing administrator credentials, VPN secrets, and authentication details.

TECHNICAL DETAILS:

SonicWall has issued a critical advisory after firewall configuration backups were leaked, potentially exposing administrator credentials, VPN secrets, and authentication details. The company strongly recommends all customers reset their login credentials and encryption keys immediately.

Organizations are urged to disable WAN management interfaces, regenerate VPN keys, reset administrator and authentication credentials, and enable enhanced logging for suspicious activity. Failure to act may allow threat actors to exploit leaked configurations to gain unauthorized access to networks.

- **Issue:** Exposure of SonicWall configuration backups has compromised sensitive system information, including administrator credentials and VPN secrets.
- **Affected Products:** SonicWall Firewalls (all models with configuration backups).
- **Risk:** Attackers may leverage leaked credentials to remotely access, modify, or exfiltrate data from internal networks.
- **Mitigation:** Implement SonicWall's recommended **containment → remediation → monitoring** approach to reduce the likelihood of exploitation.
- **Resources:** SonicWall Admin Guides and Knowledge Base articles provide step-by-step instructions for disabling WAN services, regenerating VPN keys, and resetting stored authentication secrets.

To mitigate risks, SonicWall outlines a three-phase response framework—**containment, remediation, and monitoring**—to secure impacted devices.

Containment

- Disable or restrict HTTP, HTTPS, and SSH management access over WAN.
- Restrict SSL VPN and IPsec VPN services from WAN zones.
- Block or scope inbound rules that allow WAN traffic to internal hosts.

Remediation

- Reset administrator passwords (System > Administration).
- Regenerate SSL VPN and IPsec VPN certificates, pre-shared keys, and secrets.
- Update stored credentials for LDAP, RADIUS, dynamic DNS, and wireless authentication.
- Rebind time-based one-time passwords (TOTP) in authenticator apps.
- Verify Global Management System (GMS) policies to ensure secure management access.

Monitoring

- Enable real-time firewall logging and review for:
  - Failed login attempts
  - Unexpected configuration changes
  - Unusual VPN connection patterns
- Configure alerts for repeated authentication failures and new WAN service activations.
- Integrate logs with a Security Information and Event Management (SIEM) solution.

- Maintain heightened monitoring for at least **30 days**.

RECOMMENDATIONS:

- All SonicWall customers should immediately reset credentials and implement containment measures before restoring management access.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERNCES:

- https://www.sonicwall.com/support/knowledge-base/essential-credential-reset/250909151701590