THREAT BULLETINS

UPDATE: SonicWall MySonicWall Cloud Backup Incident

TLP:WHITE

Oct 09, 2025

SonicWall recently updated its security advisory concerning the MySonicWall Cloud Backup file incident, confirming that an unauthorized party accessed firewall configuration backup files belonging to all customers who used the cloud backup service.

Health-ISAC is sharing this update to increase situational awareness and encourage organizations to assess their level of risk regarding recent developments.

Analysis

The initial disclosure of the MySonicWall Cloud Backup incident on September 17, 2025, indicated that firewall configuration files were accessed for approximately five percent of the firewall installed base. However, following a thorough investigation conducted in collaboration with security researchers, SonicWall confirmed that the scope of the breach is far broader, as an unauthorized party successfully accessed the firewall configuration backup files for every customer who had used the cloud backup feature.

To help users identify the affected products and prioritize remediation, SonicWall has updated the visibility within the MySonicWall portal. Customers must log in and navigate to the Issue List under Product Management to view a final, comprehensive list of affected serial numbers. Each listed device is assigned a priority level to guide immediate action, including:

- Active – High Priority (devices with internet-facing services enabled)
- Active – Lower Priority (devices without internet-facing services); or
- Inactive (devices that have not checked in for 90 days)

The security implications are substantial, as a firewall configuration file exposes the network's architectural blueprint and security mechanisms. This includes details like VPN pre-shared keys, administrative account names, SNMP community strings, and passwords for external integrations. Threat actors possessing this data can craft highly targeted attacks, potentially bypassing defenses to gain persistent network access, move laterally, or deploy further malicious payloads.

Recommendations and Mitigations

Health-ISAC recommends organizations review and assess their level of risk to this vulnerability and implement the following:

- Logging into your MySonicWall.com account and verify if the cloud backup fields contain details. If they are blank, you are not impacted. If details are present, check Product Management | Issue List for flagged serial numbers.
- Prioritizing remediation for devices flagged as Active – High Priority first, followed by Active – Lower Priority devices.

- Following the Essential Credential Reset guidance provided by SonicWall; this includes, but is limited to, immediately changing:
    - All local admin and local user passwords.
    - All pre-shared keys and credentials for IPSec VPN and SSL VPN.
    - All passwords/shared secrets for external authentication systems (LDAP bind accounts, RADIUS, TACACS+).
    - Passwords for external integrations (e.g., Dynamic DNS, AWS IAM keys).
- Utilizing the SonicWall Online Tool for Firewall Config Analysis to help identify services that require immediate credential remediation.
- Additional recommendations include reviewing the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Reference(s)	infosecurity-magazine, helpnetsecurity, sonicwall, bleepingcomputer, thehackernews, sonicwall 1, hhs, cyware, sonicwall 2

Alert ID fde301f3

View Alert

Share Feedback

was this helpful?  | 

Tags MySonicWall.com, SonicWall, Brute Force Attack

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

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

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/**