

THREAT BULLETINS

SonicWall MySonicWall Cloud Backup Incident



TLP:WHITE

Sep 18, 2025

SonicWall has disclosed a security incident in which threat actors gained unauthorized access to backup firewall preference files stored in its cloud service, MySonicWall.com. Although the credentials within these files were encrypted, they also contained other sensitive configuration data that could significantly facilitate future exploitation of related firewalls.

The incident is not attributed to ransomware activity but rather a series of brute force attacks aimed at gaining access to the preference files. SonicWall has prompted password resets and provided new, updated preference files to help users mitigate the potential impact.

Health-ISAC provides this information to increase situational awareness and encourage users who leverage the cloud backup feature to take immediate action to determine their exposure and mitigate any potential risk.

Analysis

The incident involved threat actors who leveraged a series of brute force attacks to gain unauthorized access to a cloud backup service.

The attackers targeted and obtained backup firewall preference files belonging to a small portion of SonicWall's customer base, specifically, less than five percent of their firewall installations. This highlights the vulnerability of cloud-based backup solutions and the importance of implementing effective security measures, as this attack specifically sought to exfiltrate sensitive configuration data.

Firewall preference files are essentially a comprehensive backup of a firewall's configuration. They contain a wide range of settings, including network configurations, security policies, and user credentials. These files allow administrators to quickly restore a firewall's settings in the event of a failure or when deploying a new device. While credentials within the files were encrypted, the files also contained other information that could potentially be used to compromise the associated firewall device.

The security implications of this breach are significant, as exposure of these files could provide attackers with critical insights into an organization's network architecture and security posture. With this information, attackers could create targeted exploits to bypass security controls, gain network access, or disrupt services. Although SonicWall has no evidence suggesting these files are being leaked online, the potential for future exploitation of affected systems remains a serious concern.

SonicWall has confirmed that this was not a ransomware event but a targeted effort to obtain configuration files for potential future use. This indicates a more sophisticated threat actor with a clear goal of gaining persistent access or leveraging the stolen data for further malicious activities. The incident serves as a crucial reminder for all organizations to regularly review their security practices and ensure that all backups, especially those stored in the cloud, are adequately protected.

Recommendations and Mitigations

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

- Implementing guidance provided by SonicWall to verify if your MySonicWall account or firewall preferences file was affected by the incident.
- Downloading and importing the updated preferences file provided by SonicWall.
- If importing the new preferences file is not feasible, manually perform the remediation steps outlined by SonicWall.
- Monitoring for potential disruption to IPSec VPN connections as importing the new preferences file may cause a firewall reboot.
- Proactively reviewing and strengthening security controls, especially for cloud-based services and backup solutions, to mitigate impacts from similar incidents.
- Reviewing the Health Industry Cybersecurity Practices (HICP): [Managing Threats and Protecting Patients Resources](#).



Reference(s)

[securityweek](#), [sonicwall](#), [sonicwall 1](#), [thehackernews](#), [infosecurity-magazine](#)

Alert ID 293a23dd

[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/>

If you are not supposed to receive this email,
please contact us at toc@h-isac.org.