CYBER ADVISORY

Tuesday, October 14, 2025 **CAL-CSIC-202510-A-002**

MySonicWall Cloud Backup File Incidents

MySonicWall	Security Breach	Firewall Config Files	Critical

SUMMARY: The California Cybersecurity Integration Center (Cal-CSIC) has identified a security breach that exposes firewall configuration backup files from MySonicWall accounts. SonicWall's investigation revealed that a threat actor could perform a series of brute for attacks against a target's MySonicWall web portal to gain access to a subset of the target's preference files stored in their cloud backups.[1] Successful security breach may expose credentials and tokens, making exploitation of firewalls significantly easier for threat actors. [2]

Affected audience:

- **Consumers who have used SonicWall's cloud backup service**

The Cal-CSIC recommends that all SonicWall customers immediately follow the guidance in the SonicWall advisory, and customers who are at-risk immediately apply the advisory's containment and remediation guidance to address the security breach.

For further information to apply upgrades please refer to the SonicWall Advisory here: MySonicWall Cloud Backup File Incident.[3]

References

[1] "SonicWall Releases Advisory for Customers after Security Incident"; "Alert"; https://www.cisa.gov/news-events/alerts/2025/09/22/sonicwall-releases-advisory-customers-after-security-incident#_ftn1; accessed 14 October 2025

[2] "SonicWall Warns Customers to Reset Credentials after Breach"; "Alert"; https://www.bleepingcomputer.com/news/security/sonicwall-warns-customers-to-reset-credentials-after-MySonicWall-breach/; accessed 14 October 2025

[3] "MySonicWall Cloud Backup File Incident";" Advisory"; https://www.sonicwall.com/support/knowledge-base/mysonicwall-cloud-backup-file-incident/250915160910330; Accessed 14 October 14, 2025