



TLP: CLEAR

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



# 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 force 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.<sup>1</sup> Successful security breach may expose credentials and tokens, making exploitation of firewalls significantly easier for threat actors.<sup>2</sup>

### 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](#).<sup>3</sup>

### References

<sup>1</sup> "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](https://www.cisa.gov/news-events/alerts/2025/09/22/sonicwall-releases-advisory-customers-after-security-incident#_ftn1); accessed 14 October 2025

<sup>2</sup> "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

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

**WARNING:** This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR