TLP:CLEAR

SonicWall Releases Advisory After Cybersecurity Incident

The United States Environmental Protection Agency (EPA) is issuing this alert to inform water and wastewater systems that are customers of SonicWall Firewalls, particularly those customers with preference files backed up on MySonicWall.com. SonicWall's security teams have recently detected suspicious activity targeting firewall preference files stored in the cloud. Although there is no current evidence of these files being leaked online by threat actors, they may contain information that could facilitate unauthorized network access by making it easier for attackers to exploit the related firewalls.

Mitigations

All water and wastewater systems that are customers of SonicWall are recommended to follow the remediation steps provided by SonicWall. Water and wastewater systems that outsource technology support are recommended to consult with their service providers for assistance with these steps.

1. Log in to your MySonicWall.com account and verify if cloud backups exist for all registered firewalls. If the fields are blank, you are not at risk.

2. If the fields contain backup details, verify whether impacted serial numbers are listed in your account. Upon login, navigate to “Product Management | Issue List” and the affected serial numbers will be flagged. If serial numbers are shown, the firewalls are at risk, and you should immediately follow the containment and remediation guidelines provided by SonicWall.

If you have used the Cloud Backup feature, but no Serial Numbers are shown, SonicWall will provide additional guidance in the coming days to determine if your backup files were impacted. Please continue to check back on the following page for additional information and updates: MySonicWall Cloud Backup File Incident.

Conclusion

If you have questions about any of the information in this alert, please contact EPA’s Water Infrastructure and Cyber Resilience Division, Cybersecurity Branch at watercyberta@epa.gov. Organizations are encouraged to report suspicious or criminal activity to the FBI Internet Crime Complaint Center (IC3) at IC3.gov or CISA via CISA’s Incident Reporting System