



Sicherheitsvorfall bei SonicWall Firewalls mit Cloud-Backup-Funktion

Der Hersteller SonicWall hat eine Sicherheitsmeldung veröffentlicht, die über einen Vorfall im Zusammenhang mit in MySonicWall gespeicherten Konfigurations-Backup-Daten informiert. Diese Daten waren unberechtigt zugänglich. Die Backups enthalten sensible Informationen, darunter verschlüsselte Zugangsdaten, deren Kenntnis Angreifern im Missbrauchsfall helfen könnte, Firewalls gezielter anzugreifen.

Um was geht es?

Der Hersteller SonicWall hat gemeldet, dass bestimmte Konfigurations-Backups von Firewalls in *MySonicWall* exponiert waren.

Im Zusammenhang mit dieser Exponierung wurden nach Angaben vom Hersteller verdächtige Aktivitäten festgestellt.

Obwohl die gespeicherten Zugangsdaten verschlüsselt sind, enthalten die Backups weitere sensible Konfigurationsinformationen, die von Angreifern missbraucht werden könnten.

Betroffen sind bestimmte Firewalls, bei denen die Funktion „Cloud Backup“ aktiviert war.

Zur Minimierung der Risiken empfiehlt SonicWall die Umsetzung konkreter Sicherheitsmassnahmen. Weitere Informationen finden Sie auch unter:

- [MySonicWall Cloud Backup File Incident](#)
- [Essential credential reset](#)
- [Remediation Playbook](#)

Update Service

Jedes System sollte regelmässig aktualisiert werden, um es gegen Schwachstellen zu schützen. Gerade bei einer Firewall empfehlen wir Ihnen regelmässige Software-Updates, da es sich um eine wichtige Sicherheitskomponente am Perimeter des Netzwerks zum Schutz ihres Netzwerkes handelt.

Mit unserem Service stellen wir sicher, dass Ihre Systeme regelmässig geprüft, optimiert und aktualisiert werden. So bleibt Ihre Netzwerksicherheit stets auf dem neuesten Stand.

Wie ist die Bedrohungslage auf meiner Anlage?

Falls Sie eine betroffene Firewall einsetzen, hängt die konkrete Bedrohungslage von Ihrer Umgebung ab. Grundsätzlich wird das Risiko als **erhöht** eingestuft, da offengelegte Konfigurationsinformationen gezielte Angriffe erleichtern können. Angreifer könnten die Informationen ausnutzen um:

- bekannte Zugangsdaten gezielt zu testen oder durch Brute-Force schneller zu kompromittieren
- Netzwerk- und VPN-Konfigurationen auszuwerten, um gezielt Schwachstellen anzugreifen
- Sicherheitsmechanismen gezielt zu umgehen, da Konfigurationseinstellungen offengelegt sein könnten

Besonders gefährdet sind Systeme, die:

- Direkten Internetzugang haben.
- Keine aktuellen Sicherheitsupdates installiert haben.
- Fehlende Schutzmechanismen wie Multi-Faktor-Authentifizierung, oder Zugriffsbeschränkungen aufweisen.

Wie kann ich mich dagegen schützen?

SonicWall empfiehlt die umgehende Umsetzung von den erwähnten Sicherheitsmassnahmen, darunter:

Credential Reset:

- Änderung aller Benutzer- und Administrator-Passwörter
- Erneuerung von VPN-Shared-Secrets und Zertifikaten
- Aktualisierung von gespeicherten Zugangsdaten in externen Diensten (LDAP, RADIUS, DDNS etc.)

Zugriffsbeschränkungen:

- Einschränkung oder Deaktivierung von SSLVPN sowie Web-/SSH-Management-Zugängen über das WAN
- Überprüfung und Absicherung aller Zugriffswege

Multi-Faktor-Authentifizierung aktivieren:

- Aktivieren Sie MFA für alle Benutzer, um unbefugten Zugriff zu verhindern

Für weitere Informationen und Unterstützung können Sie sich als Rittmeyer Kunde kostenpflichtig an unsere Hotline unter **0844 11 22 11** wenden.

