CERT.at - Show

Archived: 2026-04-05 21:33:12 UTC

20. März 2025

Beschreibung

CERT.at beobachtet weiterhin eine Welle von Ransomware-Angriffen, bei denen Cyberkriminelle bekannte kritische Schwachstellen in FortiOS- und FortiProxy-Geräten gezielt ausnutzen. Die Schwachstellen ermöglichen es Angreifern, unauthentifiziert super_admin-Rechte auf verwundbaren Geräten zu erlangen und langfristige Persistenz einzurichten.

Besonders auffällig ist, dass die Angreifer nach der erfolgreichen Infektion und Einrichtung ihrer Persistenz die Software betroffener Geräte selbst aktualisieren. Dies dient der Verschleierung und verhindert, dass weitere Angreifer dieselbe Sicherheitslücke erneut ausnutzen können. Organisationen könnten daher fälschlicherweise annehmen, dass ihre Systeme sicher und aktuell gepatcht seien, obwohl sie bereits kompromittiert sind.

CVE-Nummer(n): CVE-2024-55591, CVE-2025-24472

Auswirkungen

Angreifer können durch Ausnutzung der Schwachstellen vollständigen administrativen Zugriff auf anfällige Fortinet-Geräte erlangen. In beobachteten Angriffen erstellen die Angreifer persistente Administrator-Accounts, laden Konfigurationsdateien herunter, erlangen VPN-Zugang und bewegen sich lateral im Netzwerk. Das endgültige Ziel ist die Verbreitung von Ransomware.

Die Angriffe können zu folgenden Schäden führen:

- Vollständige Kompromittierung der Netzwerk-Sicherheitsinfrastruktur
- Datendiebstahl vor der Verschlüsselung
- Verschlüsselung von kritischen Servern und Dateien
- Erpressung durch Lösegeldforderungen

Betroffene Systeme

- FortiOS-Geräte in Versionen unterhalb von 7.0.16 mit exponierten Management-Schnittstellen, aber auch bereits gepatchte mit Persistenz

Abhilfe

CERT.at empfiehlt dringend:

- Sofortige forensische Untersuchung aller Fortinet-Geräte, die nach dem 27. Jänner 2025 noch verwundbar waren, auch wenn diese inzwischen vermeintlich gepatcht erscheinen.
- Überprüfung und Löschung unbekannter Administrator- und VPN-Konten sowie verdächtiger Automatisierungsaufgaben.
- Konsequente Beschränkung des externen Zugriffs auf Management-Schnittstellen.
- Sofortige Aktualisierung aller FortiOS-Geräte auf Versionen, die die Schwachstellen CVE-2024-55591 und CVE-2025-24472 beheben, sofern nicht bereits geschehen.

Hinweis

Wir haben die Betreiber von verwundbaren Geräten erneut über die uns bekannten Abuse-Kontakte informiert.

Generell empfiehlt CERT.at, sämtliche Software aktuell zu halten und dabei insbesondere auf automatische Updates zu setzen. Regelmäßige Neustarts stellen sicher, dass diese auch zeitnah aktiviert werden.

Informationsquelle(n):

Blog von Forescout Research - Vedere Labs (englisch)
https://www.forescout.com/blog/new-ransomware-operator-exploits-fortinet-vulnerability-duo/

Fortinet Advisory FG-IR-24-535 (englisch)
https://www.fortiguard.com/psirt/FG-IR-24-535

Source: https://www.cert.at/de/warnungen/2025/3/ransomware-gruppen-nutzen-weiterhin-kritische-fortinet-schwachstellen-warnung-vor-gepatchten-aber-bereits-kompromittierten-geraten