AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2018-13374

Auslesbare LDAP-Zugangsdaten über die REST-API von FortiOS und FortiADC.

Ein angemeldeter Administrator mit reinem Lesezugriff kann über die REST-API von FortiOS bzw. FortiADC die Verbindungsprüfung für den konfigurierten LDAP-Server auf einen eigenen, bösartigen LDAP-Server umleiten. Das Gerät sendet dabei die hinterlegten LDAP-Zugangsdaten an den Angreifer – in der Regel ein Dienstkonto des Verzeichnisdienstes. Fortinet hat die Lücke behoben; die CISA führt sie seit September 2022 als aktiv ausgenutzt.

> **Geschäftsrisiko:** Abfluss der im Gerät gespeicherten LDAP-Bind-Zugangsdaten – meist ein Konto mit Zugriff auf das Active Directory. Damit droht die Ausweitung vom Netzrand in den zentralen Verzeichnisdienst, mit Potenzial für Datenabfluss und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

4,3 / 10

MITTEL
CVSS 3.1 BASISWERT

Niedrig | **Mittel** | Hoch | Kritisch

`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N` – aus dem Netz, mit einem einfachen Read-only-Administratorkonto und ohne Zutun des Opfers – Auslesen der im Gerät hinterlegten LDAP-Zugangsdaten. Betroffen ist allein die Vertraulichkeit; Integrität und Verfügbarkeit bleiben unberührt. CVSS 2.0 bewertet die Lücke mit 4,0.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
8. September 2022	FortiOS ≤ 6.0.2 · FortiADC 5.4.0-5.4.4, 6.0.0-6.0.1, 6.1.0	Zeitnah

Das Wichtigste in 60 Sekunden.

4,3 · MITTEL
CVSS-Schweregrad (3.1)

Read-only
angemeldetes Lesekonto genügt

CISA KEV
aktiv ausgenutzt · seit 08.09.2022

CWE-732
falsche Rechtevergabe

Die Ursache: FortiOS und FortiADC bieten in der Administrationsoberfläche eine Funktion, um die Verbindung zum konfigurierten LDAP-Server zu testen. In den betroffenen Versionen dürfen auch **Administratoren mit reinem Lesezugriff** die Zieladresse dieses Tests über die REST-API verändern. Wird der Test auf einen vom Angreifer kontrollierten **Rogue-LDAP-Server** umgeleitet, übermittelt das Gerät die hinterlegten LDAP-Bind-Zugangsdaten dorthin – und gibt sie damit preis.

ANGRIFFSKETTE

01
Zugang mit Lesekonto – der Angreifer verfügt über ein Read-only-Administratorkonto oder erreicht die Management-API

02
LDAP-Test umbiegen – die Server-Konnektivitätsprüfung per REST-API auf einen eigenen, bösartigen LDAP-Server richten

03
Zugangsdaten abgreifen – das Gerät sendet die konfigurierten LDAP-Bind-Credentials an den Rogue-Server

04
Ausweitung – mit dem erbeuteten Verzeichnis-Dienstkonto weiter ins Active Directory / den LDAP-Verzeichnisdienst vordringen

Betroffenheit & Fixversionen

Produkt / Version	Verwundbar bis	Fixversion (Ziel)
FortiOS	5.6.7 und früher · 6.0.0-6.0.2	6.0.3
FortiADC 6.1	6.1.0	6.1.1
FortiADC 6.0	6.0.0-6.0.1	6.0.2
FortiADC 5.4	5.4.0-5.4.4	5.4.5

Betroffen sind FortiOS bis einschließlich 6.0.2 sowie die genannten FortiADC-Zweige. FortiOS 6.0.3 und höher (bzw. 6.2.0) beheben die Schwachstelle. Die Ausnutzung setzt ein angemeldetes Administratorkonto voraus – auch ein reines Read-only-Konto genügt, weshalb kompromittierte oder zu großzügig vergebene Lesekonten das eigentliche Einfallstor sind.

Regulatorischer Hinweis: Fließen über diese Lücke LDAP-Zugangsdaten und in der Folge Verzeichnis- bzw. personenbezogene Daten ab, kann eine meldepflichtige Verletzung vorliegen – DSGVO unverzüglich (i. d. R. 72 h), NIS-2 nach den für Sie geltenden Fristen. Die Meldung bleibt bei Ihnen; wir unterstützen bei Bewertung und Dokumentation.

ZEITACHSE

Nov. 2018
CVE-2018-13374 wird veröffentlicht

01.06.2021
Fortinet veröffentlicht Advisory FG-IR-18-157 mit Fixversionen

08.09.2022
CISA nimmt CVE-2018-13374 in den KEV-Katalog auf – aktive Ausnutzung

29.09.2022
KEV-Frist für US-Behörden zum Patchen

Ihr Maßnahmenplan.

In dieser Reihenfolge – patchen, Zugriff und Lesekonten härten, LDAP-Zugangsdaten rotieren, Missbrauch ausschließen.

SOFORT	KURZFRISTIG	PARALLEL
Fixversion einspielen	LDAP-Bind-Zugangsdaten rotieren	Adminkonten & Verzeichnis-Logs prüfen

01 Betroffenheit feststellen

Prüfen, ob FortiOS in einer Version bis einschließlich `6.0.2` oder ein betroffener FortiADC-Zweig (`5.4.0-5.4.4`, `6.0.0-6.0.1`, `6.1.0`) im Einsatz ist und ob ein LDAP-Server (z. B. Active Directory) im Gerät konfiguriert ist.

02 Patchen

FortiOS auf `6.0.3` oder neuer aktualisieren; FortiADC auf `5.4.5`, `6.0.2` bzw. `6.1.1` oder neuer. Damit ist die unberechtigte Änderung des LDAP-Testziels geschlossen.

03 Management-Zugriff und Lesekonten härten

Die Administrations- und REST-API-Schnittstelle nicht aus dem Internet erreichbar machen, auf autorisierte Hosts/Netze begrenzen und Read-only-Administratorkonten nach dem Least-Privilege-Prinzip auf das Nötige beschränken. Die Ausnutzung setzt ein angemeldetes Konto voraus.

04 LDAP-Zugangsdaten als kompromittiert behandeln

Das im Gerät hinterlegte LDAP-Bind-Konto rotieren (neues Passwort) – ein Patch macht bereits abgeflossene Zugangsdaten nicht ungültig. Handelt es sich um ein Dienstkonto mit weitreichenden AD-Rechten, dessen Rechte zusätzlich einschränken.

05 Missbrauch ausschließen

Verzeichnisdienst- bzw. Domänencontroller-Logs auf ungewöhnliche Anmeldungen des LDAP-Bind-Kontos prüfen und die Konfigurations- sowie Zugriffslogs der FortiGate/FortiADC auf Änderungen am LDAP-Testziel und auf verdächtige API-Aufrufe durchsehen.

Kompromittierungs-Indikatoren (IoCs)

KONFIGURATIONS-CHECK

Änderungen am hinterlegten LDAP-Server-Ziel
oder API-Aufrufe der LDAP-Testfunktion
durch Read-only-Konten

AUFFÄLLIGE AKTIVITÄT

Ausgehende LDAP-Bind-Versuche der FortiGate
zu unbekannten, externen Zieladressen

FOLGEINDIKATOREN

Anmeldungen des LDAP-Bind-/Dienstkontos
an Domänencontrollern von fremden Quellen

Zur Einordnung: Da die Schwachstelle über eine legitime Verwaltungsfunktion und ein angemeldetes Konto ausgenutzt wird, hinterlässt sie kaum eindeutige Netz-IOCs. Der zuverlässigste Nachweis ist die Auswertung Ihrer Geräte-Audit-Logs (Änderungen am LDAP-Testziel) sowie der Anmelde-Logs des betroffenen Verzeichnis-Dienstkontos.

Wichtig: Der Kern des Risikos liegt nicht im FortiGate selbst, sondern im dort hinterlegten LDAP-Dienstkonto: Ist dessen Passwort einmal abgeflossen, bleibt der Zugang zum Verzeichnisdienst auch nach dem Patch bestehen. Deshalb ist die Rotation der LDAP-Bind-Zugangsdaten ebenso wichtig wie das Update.

Lassen Sie das von unseren Experten prüfen.

Drei Bausteine, die genau auf diese Schwachstelle einzahlen – vom schnellen Exposure-Check bis zur laufenden Absicherung.

Cyber Defense Center

24/7-SOC aus München: Änderungen am LDAP-Testziel durch Read-only-Konten und die anschließende Nutzung abgeflossener Verzeichnis-Zugangsdaten fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden erreichbare, ungepatchte FortiOS-/FortiADC-Management-Schnittstellen mit konfiguriertem LDAP-Server über Ihren gesamten Perimeter – bevor Angreifer sie finden – und priorisieren nach realer Ausnutzung.

Incident-Response-Retainer

Bei Verdacht auf einen bereits erfolgten Zugriff übernimmt unser IR-Team Forensik und Eindämmung – mit vertraglich zugesicherter Reaktionszeit.

SO GEHEN WIR VOR

01 Exposure-Check

Wir prüfen, ob Ihre FortiOS / FortiADC-Systeme verwundbar konfiguriert und exponiert sind.

02 Sofortmaßnahmen begleiten

Mitigation und Patch-Fahrplan gemeinsam mit Ihrem Team umgesetzt.

03 Absichern & überwachen

Threat Hunting auf die IoCs, danach laufendes Monitoring und IR-Bereitschaft – 24/7, wenn Ihr Team das nicht selbst leisten kann.

Empfehlung für die Geschäftsleitung

- FortiOS/FortiADC unverzüglich auf die genannten Fixversionen aktualisieren und die Management-Schnittstelle vom Internet trennen.
- Das im Gerät hinterlegte LDAP-Bind-Konto rotieren und seine AD-Rechte auf das Nötige beschränken lassen.
- Prüfen lassen, ob das Verzeichnis-Dienstkonto bereits missbraucht wurde – dokumentiert für eine etwaige Meldung.

Ihr Part · unser Part. Sie behalten die Kontrolle über Konfiguration und Freigaben; wir liefern Analyse, Bewertung und – im Retainer – die Reaktionskette.

Rollen, Eingriffstiefe und SLAs im Erstgespräch (RACI, AVV/TOM auf Anfrage) · Datenhaltung auf Wunsch vollständig in Deutschland · ISO/IEC 27001 (TÜV SÜD) · deutschsprachige Analysten.

Sprechen Sie mit uns, bevor es ein Angreifer tut.

Kostenloses 30-Minuten-Erstgespräch – wir prüfen Ihre Exposure gegenüber CVE-2018-13374 und dem FortiOS / FortiADC-Perimeter.

+49 89 45 24 24-100 · kontakt@argos.security · www.argos.security

Termin buchen

Quellen: Fortinet PSIRT Advisory FG-IR-18-157 (Fixversionen FortiOS 6.0.3; FortiADC 5.4.5 / 6.0.2 / 6.1.1) · NVD (CVSS 3.1: 4,3 MITTEL, Vektor AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N; CVSS 2.0: 4,0; CWE-732) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 08.09.2022, Frist 29.09.2022). Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversion gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.