AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2019-5591

Standardkonfiguration ohne Server-Identitätsprüfung in Fortinet FortiOS.

In der Standardkonfiguration prüft FortiOS die Identität des LDAP-Servers nicht. Ein nicht authentifizierter Angreifer im selben Subnetz kann sich dadurch als LDAP-Server ausgeben, den Authentifizierungsverkehr abfangen und sensible Informationen – darunter Zugangsdaten – mitlesen (Man-in-the-Middle). Die Schwachstelle steht auf der CISA-KEV-Liste und wurde im Verbund mit weiteren FortiOS-Lücken von APT-Gruppen aktiv ausgenutzt.

Geschäftsrisiko: Abgreifen von LDAP-Verzeichnis- und Anmeldeinformationen durch einen Angreifer im lokalen Netz und in der Folge unbefugter Zugriff auf angebundene Systeme – mit Potenzial für Datenabfluss, laterale Ausbreitung und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

6,5 / 10

MITTEL
CVSS 3.1 BASISWERT

Niedrig | **Mittel** | Hoch | Kritisch

`CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N` – aus dem angrenzenden Netz (gleiches Subnetz), ohne Anmeldung und ohne Zutun eines Nutzers – vollständiger Zugriff auf abgefangene, vertrauliche Authentifizierungsdaten. Der ältere CVSS-2.0-Wert liegt bei 3,3.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
April 2021 (FBI/CISA-Warnung vor APT-Ausnutzung)	FortiOS ≤ 6.2.0 (LDAP/FSSO ohne server-identity-check)	Hoch

Das Wichtigste in 60 Sekunden.

6,5 · MITTEL
CVSS-Schweregrad (3.1)

Adjacent
gleiches Subnetz, ohne Anmeldung

Aktiv
ausgenutzt · CISA KEV (seit 03.11.2021)

CWE-306
Fehlende Authentisierung

Die Ursache: FortiOS überprüft in den betroffenen Versionen in der **Standardkonfiguration** die Identität des angebundenen LDAP-Servers nicht – die Option `server-identity-check` ist nicht aktiv. Ein **nicht authentifizierter** Angreifer im selben Subnetz kann sich dadurch als LDAP-Server ausgeben, die Verbindung auf sich umleiten und den zur Authentifizierung übertragenen Datenverkehr abfangen und mitlesen (Man-in-the-Middle). Ursache ist eine unsichere Voreinstellung, kein Programmierfehler.

ANGRIFFSKETTE

01
Position im Netz – der Angreifer befindet sich im selben Subnetz wie die FortiGate

02
LDAP-Server vortäuschen – er gibt sich als der erwartete LDAP-/FSSO-Server aus, da FortiOS dessen Identität nicht prüft

03
Verkehr abfangen – der Authentifizierungsverkehr wird umgeleitet und mitgelesen; sensible Informationen und Zugangsdaten fließen ab

04
Ausweitung – erbeutete Verzeichnis-/Anmeldeinformationen werden für Zugriff auf angebundene Systeme und laterale Bewegung genutzt

Betroffenheit & Fixversionen

FortiOS-Version	Verwundbar bis	Fixversion (Ziel)
FortiOS (LDAP/FSSO)	≤ `6.2.0`	`6.2.1`
FortiOS 6.2.1 und neuer	nur bei aus Alt-Version übernommener Einstellung	server-identity-check aktivieren

Betroffen ist FortiOS in allen Versionen bis einschließlich `6.2.0`, sofern LDAP-/FSSO-Authentifizierung ohne aktivierte Server-Identitätsprüfung genutzt wird. Ab `6.2.1` ist `server-identity-check` bei einer Neuinstallation standardmäßig aktiv – **ein Firmware-Upgrade allein schließt die Lücke jedoch nicht**: aus Kompatibilitätsgründen bleibt der bestehende Wert der Einstellung beim Update unverändert und muss aktiv geprüft und gesetzt werden.

Regulatorischer Hinweis: Werden über den abgefangenen Verkehr Zugangsdaten oder personenbezogene Daten kompromittiert, kann dies eine meldepflichtige Verletzung darstellen – 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

26.07.2019
Fortinet veröffentlicht Advisory FG-IR-19-037 mit Abhilfe (server-identity-check)

02.04.2021
FBI/CISA warnen in gemeinsamem Advisory vor APT-Ausnutzung von FortiOS-Lücken inkl. CVE-2019-5591

03.11.2021
CISA nimmt CVE-2019-5591 in den KEV-Katalog auf – bekannte Ausnutzung

03.05.2022
KEV-Frist für US-Behörden zur Umsetzung der Herstellervorgaben

Ihr Maßnahmenplan.

In dieser Reihenfolge – Betroffenheit prüfen, Server-Identitätsprüfung aktivieren, aktualisieren und Einstellung verifizieren, Zugangsdaten absichern.

SOFORT	KURZFRISTIG	PARALLEL

01 Betroffenheit feststellen

Prüfen, ob FortiOS in einer Version bis einschließlich `6.2.0` im Einsatz ist und ob LDAP- bzw. FSSO-Authentifizierung genutzt wird. Auch bereits aktualisierte Systeme prüfen – die Einstellung wird beim Upgrade nicht automatisch gesetzt.

02 Server-Identitätsprüfung aktivieren

Die von Fortinet benannte Abhilfe umsetzen: für jeden LDAP-Server sichere Verbindung, CA-Zertifikat und `server-identity-check` setzen. Damit ist die Lücke unabhängig von der FortiOS-Version geschlossen.

```
config user ldap edit "ldap-server" set
ca-cert <ldap-server-certificate> set
secure ldaps set server-identity-check
enable next end
```

03 Aktualisieren und Einstellung verifizieren

Auf eine aktuelle, vom Hersteller unterstützte FortiOS-Version aktualisieren (ab `6.2.1` ist die Prüfung bei Neuinstallation Standard). Nach dem Update zwingend kontrollieren, dass `server-identity-check` tatsächlich aktiv ist – der Wert bleibt beim Upgrade unverändert.

04 Zugangsdaten absichern

Da über die Lücke Authentifizierungsverkehr abgefangen werden konnte, betroffene LDAP-/Verzeichnis- und Dienstkonten als potenziell kompromittiert behandeln und die Zugangsdaten rotieren – die Behebung macht bereits abgeflossene Geheimnisse nicht ungültig.

05 Netzexposition reduzieren

Der Angriff erfordert eine Position im selben Subnetz. Managementebene und LDAP-/FSSO-Kommunikation in vertrauenswürdige, segmentierte Netze verlagern und den Zugriff auf autorisierte Hosts begrenzen.

Kompromittierungs-Indikatoren (IoCs)

KONFIGURATIONS-CHECK

`server-identity-check` je LDAP-Server
`show user ldap`

AUFFÄLLIGE AKTIVITÄT

Unerwartete ARP-/LDAP-Antworten oder ein
zweiter, unbekannter LDAP-Endpunkt im Subnetz

FOLGEINDIKATOREN

Anmeldungen mit LDAP-Konten aus untypischer
Quelle oder zu ungewöhnlichen Zeiten

Zur Einordnung: Ein aktiver Man-in-the-Middle hinterlässt auf der FortiGate selbst kaum Spuren. Der belastbarste Nachweis ist der Konfigurationszustand (server-identity-check aktiv?); ein zurückliegender Angriff lässt sich meist nur über Netz-/Verzeichnis-Logs und ungewöhnliche Anmeldemuster rekonstruieren.

Wichtig: Der Kern des Risikos ist die unsichere Voreinstellung: Ein Firmware-Upgrade allein behebt die Lücke nicht, weil FortiOS den bestehenden Wert von server-identity-check beim Update aus Kompatibilitätsgründen beibehält. Entscheidend ist, die Server-Identitätsprüfung aktiv zu setzen und nach jedem Update zu verifizieren.

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: Auffällige LDAP-Antworten im Subnetz und Anmeldungen mit über den abgefangenen Verkehr erlangten Verzeichniskonten fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden FortiGate-Systeme mit LDAP-/FSSO-Anbindung ohne aktivierte Server-Identitätsprüfung 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-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

- server-identity-check auf allen FortiGate-Systemen mit LDAP-/FSSO-Anbindung heute aktivieren und auch nach Upgrades verifizieren lassen.
- Betroffene LDAP-/Dienstkonten als potenziell kompromittiert behandeln und Zugangsdaten rotieren.
- Management- und Authentifizierungsverkehr in segmentierte, vertrauenswürdige Netze verlagern, um Angreifer im gleichen Subnetz auszuschließen.

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-2019-5591 und dem FortiOS-Perimeter.

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

Termin buchen

Quellen: Fortinet PSIRT Advisory FG-IR-19-037 (veröffentlicht 26.07.2019, Abhilfe server-identity-check, ab FortiOS 6.2.1 Standard bei Neuinstallation) · NVD (CVSS 3.1: 6,5 MITTEL, Vektor AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N; CVSS 2.0: 3,3; CWE-306) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 03.11.2021, Frist 03.05.2022) · FBI/CISA Joint Advisory vom 02.04.2021 zur APT-Ausnutzung von FortiOS-Schwachstellen. Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversion und Konfiguration gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.