IF TECH AG
part of connexta

Compliant Device Bypass

Schwachstelle in CA-Richtlinien

Version: 1.0

Datum: 14.01.2025

T +49 89 2000669-10
E info@if-tech.de
W www.if-tech.de

A IF-Tech AG
Willy-Brandt-Allee 4
81829 München

Registergericht München
HRB 184376
Ust-Id: DE270290273

Teil der connexta - IT-Gruppe Mittelstand
Vorsitzender des Aufsichtsrats: Dr. Jens Stief;
Vorstand: Marco Klose, Hans-Jörg Friedrich, Marcus Junker

Was steckt hinter Compliance ByPass?

Diese Schwachstelle ermöglicht es Angreifern, die Abfrage des „Compliant-Status“ von Geräten zu umgehen und somit Schutzmechanismen, wie Conditional-Access auszusetzen.

Durch die Extraktion von Token, die normalerweise für die Intune-Company-Portal-App bestimmt sind, kann ein Angreifer den „Compliant-Device“ Status auf einem unbekannten Gerät erlangen, und somit Conditional-Access Richtlinien, die ein Compliant-Device erfordern umgehen.

Wie läuft ein Angriff ab?

Angreifer können Tokens aus der Intune-Company-Portal-App extrahieren und für andere Microsoft-Anwendungen verwenden, wodurch Device-Compliance-Prüfungen umgangen werden können.

Durch die Nutzung einer speziellen URL und Tools wie TokenSmith kann dieser Angriff schnell reproduziert werden, was einen Angriffsversuch verhältnismäßig leicht macht.

Welche Risiken eröffnet die Sicherheitslücke?

Mit Hilfe von Conditional-Access kann der Zugriff auf Unternehmensressourcen individuell gesteuert werden. So kann ein Unternehmen z.B. den Zugriff auf Daten ohne MFA erlauben, wenn das Gerät im Tenant bekannt ist und dieses den „Compliant-Status“ aufweist.

Dadurch, dass nun die Device-Status-Abfragen umgangen werden kann, können Angreifer an Conditional-Access vorbei Sign-In Versuche am Tenant ohne Multi-Faktor-Authentifizierung durchführen

Welche Maßnahmen können schnell getroffen werden?

Wir empfehlen, für sämtliche Zugriffe (insbesondere für Anmeldungen an der Company-Portal-App) Multi-Faktor-Authentifizierung anzufordern.

Zudem sollten Sie prüfen, ob Sie über CA-Richtlinien Anmeldungen ohne MFA zulassen, wenn das Gerät den „Compliant-Status“ entspricht.

Um die Sicherheitslücke vorläufig komplett selbständig zu schließen, können Sie eine Block-Regel in Conditonal Access erstellen, die sämtliche Zugriffe von nicht in „Entra-ID joined“ bzw. „Hybrid-Joined Devices“ blockiert. Hierfür können Sie auf einen Devicefilter (*device.trustType -eq "AzureAD" -or device.trustType -eq "ServerAD")* zurückgreifen. **Beachten Sie jedoch, dass dies zur Folge hat, dass auch keine neuen Devices im Tenant registriert werden können. Hier wären dann ggf. temporäre Ausnahmen für das Enrollment neuer Geräte nötig. Zugriffe von privaten Devices ist dann nicht mehr möglich.**

Prävention durch Sentinel oder SIEM-Lösungen möglich?

Microsoft Sentinel kann die Anmeldeprotokolle im Tenant analysieren, und somit mit Hilfe von Detection Rules erkennen, ob versucht wird, die Schwachstelle auszunutzen. Anschließen könnte mit automatisieren Playbooks der Zugang des betroffenen Users gesperrt werden.

Mit folgender KQL Query könne Sie ihre SignIn-Logs auf mögliche erfolgreiche Zugriffe über die Company-Portal-Schwachstelle durchsuchen:

```
SigninLogs

| where AppId == "9ba1a5c7-f17a-4de9-a1f1-6178c8d51223"
and ResourceDisplayName == "Microsoft Graph"
and ResultType == "0" // => Successful SignIns
and TimeGenerated >= ago(90d)

| extend devices = parse_json(DeviceDetail)
| extend CAP = parse_json(ConditionalAccessPolicies)

| mv-expand CAP
| where (CAP.enforcedGrantControls has "RequireCompliantDevice" and CAP.result == "failure") or (CAP.enforcedGrantControls has "Block" and CAP.result == "notApplied")
```

Wo liegt die Gefahr & wer ist gefährdet?

Mit Hilfe der Schwachstelle können Angreifer solche Conditional-Access Regeln umgehen, die einem „Compliant-Device“ vertrauen.

Bestehen bleibt jedoch die Hürde, dass der Angreifer gültige Zugangsdaten (Benutzername & Passwort) sowie MFA (falls angefordert) für den Ziel-Tenant benötigen.

Zudem benötigt der Angreifer auch noch den hier mehrmals thematisierten Token.