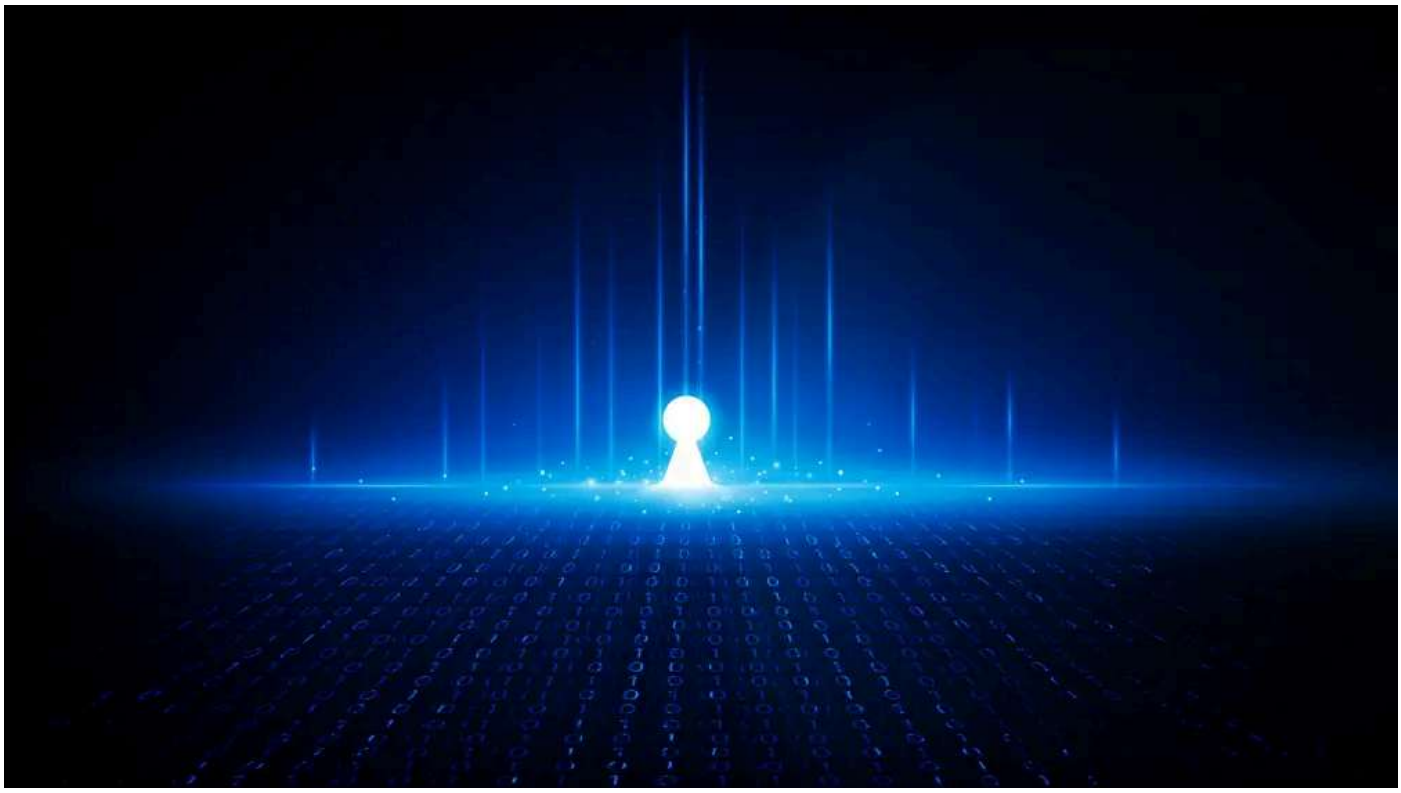
Kritische Entra-ID-Lücke machte alle Tenants global kompromittierbar

Aufgrund einer Schwachstelle in Entra ID hätten Angreifer als Admin auf beliebige Tenants zugreifen können. Das Sicherheitsproblem ist schon länger gelöst.



(Bild: RaiDztor/Shutterstock.com)

19.09.2025, 10:36 Uhr **Lesezeit: 2 Min.** | **Security**

Von Dennis Schirrmacher

Microsofts Identitäts- und Zugriffsverwaltungsdienst Entra ID war kaputt. Angreifer hätten mit vergleichsweise wenig Aufwand an einer "**kritischen**" Sicherheitslücke ansetzen können. Davon waren global alle Entra-ID-Tenants betroffen. Microsoft hat die Schwachstelle im Juli dieses Jahres geschlossen. Nun führt ein Sicherheitsforscher Hintergründe zur Lücke aus.

Durch das erfolgreiche Ausnutzen der Schwachstelle war ein Admin-Zugriff auf beliebige Tenants möglich. Weil weltweit unter anderem große Unternehmen Entra ID nutzen, hätten Attacken weitreichende Folgen haben können.

Hintergründe

In einem ausführlichen Beitrag erläutert ein Sicherheitsforscher von Outsidersecurity das Sicherheitsproblem. Er gibt an, die "**kritische**" Schwachstelle (CVE-2025-55241) mit Höchstwertung (CVSS Score 10 von 10) im Juli dieses Jahres entdeckt und umgehend an Microsoft gemeldet zu haben. Er schreibt, dass Microsoft die Schwachstelle innerhalb weniger Tage geschlossen hat. Dafür mussten Entra-ID-Tenants nichts tun. Offensichtlich wurde das Problem serverseitig gelöst.

Um die Lücke auszunutzen, mussten Angreifer aber die Tenant-ID und die NetID eines Nutzers kennen. Doch beides lässt sich dem Forscher zufolge mit vergleichsweise wenig Aufwand herausfinden. Dass das keine so große Hürde sein kann, unterstützt auch die kritische Einstufung der Schwachstelle.

Dem Sicherheitsforscher zufolge fußt eine Attacke auf zwei Grundlagen: Der erste Ansatzpunkt ist ein undokumentierter Token zur Identitätsfeststellung mit der Bezeichnung "Actor Token". Diesen nutzt Microsoft in seinem Backend für Service-to-Service-Kommunikation.

Die zweite Komponente ist die eigentliche Schwachstelle in der Azure AD Graph API (Legacy), die solche Tokens nicht ausreichend überprüft. Demzufolge hätten sich Angreifer damit ausgerüstet als Admin für beliebige Tenants ausgeben können. Der Sicherheitsforscher führt aus, dass diese Tokens aufgrund ihrer Beschaffenheit an allen Sicherheitsrichtlinien vorbeischlüpfen, sodass es keine Gegenmaßnahme gab.

Nach erfolgreichen Attacken hätten Angreifer vollen Zugriff auf Entra-ID-Tenants gehabt. So hätten sie unter anderem persönliche Informationen und BitLocker-Schlüssel einsehen und die volle Kontrolle über Services wie SharePoint Online erlangen können. Erschwerend kommt hinzu, dass ein Angreifer mit einem Actor Token keine Spuren in Logs hinterlässt.

Microsoft gibt an, dass ihnen keine derartigen Attacken bekannt sind. Der Sicherheitsforscher führt in seinem Bericht weitere technische Hintergründe aus. In einer Warnmeldung listet Microsoft weitere Details auf.

(des)

MEHR ZUM THEMA

Immer informiert bleiben: Klicken Sie auf das Plus-Symbol an einem Thema, um diesem zu folgen. Wir zeigen Ihnen alle neuen Inhalte zu Ihren Themen.
Mehr erfahren.

Entra ID | IT | Microsoft | Security | Sicherheitslücken

TEILE DIESEN BEITRAG

Kurzlink: https://heise.de/-10662375

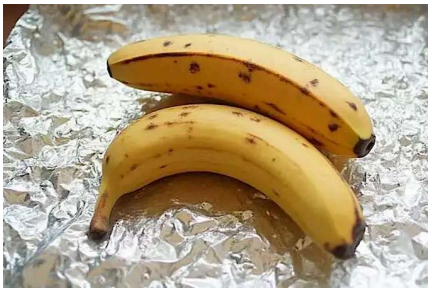
Windows 11: Altes Kontextmenü...
tipps + tricks

Telekom und Vodafone müss...
heise online

Mit Batterien aus alten E-...
heise online

Amazon-Lieferdrohne...
heise online

Milben nisten sich unbemerkt im Bett ei...
Med Direkt



Schlechter Stuhlgang bei Senioren: Diesen...
Floravia

Baden-württemberg beschließt neues...
1komma5.com

Nach der Zerschlagung eines Cybercrime-Netzwerks erklären wir, wie die Täter genau vorgingen und was Verbraucher wissen und worauf sie achten sollten.

News

Apples iPhone-Geschäft läuft gut – aber welches kaufen?

Apple erwartet zum Weihnachtsgeschäft die bislang besten iPhone-Verkäufe aller Zeiten. Für Käufer wird es aber immer unübersichtlicher.

News

US-Patentamt ändert Regeln für KI-gestützte Erfindungen

Das US-Patentamt hat festgelegt, wie mithilfe von KI entwickelte Erfindungen gewerblich geschützt werden können. Eine natürliche Person muss im Spiel sein.

Hintergrund

Bahn-Chaos und Verspätungen: Warum die Sanierung der Gleise allein nicht hilft

Überall wird bei der Bahn gebaut. Doch an vielen Problemen des Schienennetzes ändert das langfristig wenig. Warum das so ist und was man besser machen könnte.

Wero ist im Onlinehandel gestartet. Wir geben einen aktuellen Überblick zum Stand des europäischen Bezahlsystems und haben es im Shop ausprobiert.

News

Raspberry-Pi-Projekte fürs Netz – NAS, Cloud & Router selbst gebaut | c’t uplink

Der Raspberry Pi eignet sich für vieles: Opencloud-Host, Selbstbau-NAS oder als OpenWRT-Router. Die Vorteile davon und wie das geht, erklären wir in c’t uplink.

Beliebte Bestenlisten

Letzte Chance für Top-Angebote zum Finale der Black Week

bestenlisten

Weder Apple noch Nintendo: Die beliebtesten Black-Friday-Deals

bestenlisten

Die besten Black-Friday-Angebote für Laptops & Mini-PCs

bestenlisten

Alle bestenlisten →