Fehlerbehebung: Browser-basierte Secure Access-SAML-Authentifizierung mit leerem Weißbildschirm mit EntraID

Inhalt

Problem

Wenn Sie Cisco Secure Access so konfigurieren, dass auf Geräten ohne installierten Cisco Secure Client eine browserbasierte SAML-Authentifizierung erzwungen wird, wird statt der EntraID-Authentifizierungsseite auf einen leeren weißen Bildschirm umgeleitet. Dieses Problem tritt speziell im normalen Microsoft Edge-Modus (nicht inPrivate) und in Google Chrome-Browsern auf. Die Authentifizierung funktioniert ordnungsgemäß, wenn der Edge InPrivate-Modus verwendet wird. Im SAML-Authentifizierungsprofil sind sowohl Entschlüsselung als auch SSO-Authentifizierung aktiviert.

Die konfigurierte Richtlinienstruktur umfasst:

- Richtlinien für Benutzer nach der Authentifizierung zulassen. (Quelle: Jeder Benutzer, Ziel: any)
- SAML-Authentifizierungsrichtlinie mit SAML-Authentifizierungsprofil zulassen. (Quelle: Endpunkt-IP, Ziel: 0.0.0.0 TCP 80, 443)
- SAML-Authentifizierungshelferrichtlinie mit SAML-Authentifizierungsprofil zulassen. (Quelle: Endpunkt-IP, Ziel: any)
- Blockieren von Richtlinien. (Quelle: Endpunkt-IP, Ziel: any)

Umwelt

- Cisco Secure Access (Internetzugangsmodul)
- EntraID als Identitätsanbieter (IdP)

- Browserbasierte SAML-Authentifizierung für Geräte ohne Cisco Secure Client
- SAML-Authentifizierungsprofil mit aktivierter Entschlüsselung und SSO-Authentifizierung
- Browser Microsoft Edge und Google Chrome

Auflösung

Das Problem wird behoben, indem der Entschlüsselungsausschlussliste in der Konfiguration des SAML-Authentifizierungsprofils bestimmte EntraID-bezogene Domänen hinzugefügt werden. Dadurch wird verhindert, dass der SSL/TLS-Entschlüsselungsprozess den EntraID-Authentifizierungsablauf beeinträchtigt.

Schritt 1: EntraID-Domänen zur Entschlüsselungsausschlussliste hinzufügen

Konfigurieren Sie diese vier EntraID-Domänen in der Entschlüsselungsausschlussliste für das SAML-Authentifizierungsprofil:

```
login.live.com
login.microsoftonline.com
msauth.net
msftauth.net
```

Phase 2: Konfiguration auf SAML-Richtlinien anwenden

Stellen Sie sicher, dass die Einstellungen für den Entschlüsselungsausschluss auf beide angewendet werden:

- Die Richtlinie SAML-Authentifizierung zulassen. (Quelle: Endpunkt-IP, Ziel: 0.0.0.0 TCP 80, 443)
- Die Richtlinie SAML-Authentifizierungshilfe zulassen. (Quelle: Endpunkt-IP, Ziel: any)

Schritt 3: Auflösung überprüfen

Nachdem Sie die Entschlüsselungsausschlusskonfiguration angewendet haben, testen Sie den Authentifizierungsablauf:

- Microsoft Edge (Normalmodus): Die Umleitung zur EntraID-Authentifizierungsseite ist erfolgreich.
- Google Chrome: Die Umleitung zur EntraID-Authentifizierungsseite ist erfolgreich.
- Beide Browser können den Eingabebildschirm für die EntraID-Authentifizierung durchgängig anzeigen.

Ursache

Der leere weiße Bildschirm wird angezeigt, weil der SSL/TLS-Entschlüsselungsprozess in Cisco Secure Access den EntraID-Authentifizierungsablauf beeinträchtigt, wenn die Entschlüsselung für das SAML-Authentifizierungsprofil aktiviert ist. Der Entschlüsselungsvorgang unterbricht die sichere Kommunikation zwischen dem Browser und den EntraID-Authentifizierungsservern, sodass die Authentifizierungsseite nicht ordnungsgemäß geladen wird. Der InPrivate-Modus funktioniert, da SSL/TLS-Sitzungen anders behandelt werden und die Entschlüsselungsinterferenz umgangen wird. Durch das Hinzufügen der EntraID-Domänen zur Entschlüsselungsausschlussliste kann der Authentifizierungsverkehr ohne Entschlüsselung weitergeleitet werden, wobei die Integrität des sicheren Authentifizierungsflusses erhalten bleibt.

Verwandte Inhalte

- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.