Fehlerbehebung bei SWG-SAML-Authentifizierungscookie-Surrogat-Problem für sicheren Zugriff

Inhalt

Problem

Benutzer, die über Cisco Secure Access auf Webanwendungen zugreifen, haben Authentifizierungsfehler, wenn Anwendungen domänenübergreifende Umleitungen durchführen oder Ressourcen von mehreren verwandten Domänen abrufen. Das Problem äußert sich wie folgt:

- Webanwendungen können nach der SAML-Authentifizierung nicht ordnungsgemäß initialisiert werden.
- Anforderungen an domänenübergreifende Ressourcen (CORS-Fehler), die standardmäßig blockiert werden, verweigern Regeln.
- Aktivitätsprotokolle, in denen Anforderungen angezeigt werden, die der Netzwerk- oder Tunnelidentität anstelle der authentifizierten Benutzeridentität zugeordnet sind.
- CORS-Richtlinienfehler werden in der Browserkonsole für umgeleitete Anfragen angezeigt.
- Anwendungen arbeiten korrekt auf physischen Computern, wenn IP-Surrogat verwendet wird, aber in Citrix Virtual Desktop-Umgebungen mit Cookie-Surrogat ausfällt.

Das Problem tritt insbesondere dann auf, wenn die Cookie-Surrogat-Authentifizierung in virtualisierten Umgebungen verwendet wird, in denen umgeleitete Anforderungen die Zuordnung von Benutzer zu Cookie während domänenübergreifender Ressourcenabrufe verlieren.

Umwelt

- Cisco Secure Access mit konfigurierter SAML-Authentifizierung
- Cookie-Ersatz-Authentifizierung für virtuelle Citrix Desktop-Umgebungen aktiviert

- IP-Surrogat-Authentifizierung für physische Systeme
- Webanwendungen, die domänenübergreifende Umleitungen ausführen (CORS-Fehler in Konsolenprotokollen des Webentwicklungstools)
- Gemischte Umgebung mit physischer und virtueller Desktop-Infrastruktur

Auflösung

Das Problem wird durch die Implementierung von IP-Surrogat-Bypass für die betroffenen Netzwerkbereiche gelöst, sodass die Benutzeridentität auch bei domänenübergreifenden Umleitungen korrekt zugewiesen werden kann.

Schritt 1: Zur IP-Ersatzkonfiguration navigieren

Rufen Sie das Cisco Secure Access-Dashboard auf, und navigieren Sie zu Verbinden > Benutzer und Gruppen > Konfigurationsmanagement > Erweiterte Einstellungen > IP-Ersatz.

Phase 2: Umgehung des internen Netzwerks aktivieren

Fügen Sie die betroffenen Netzwerkbereiche zur Umgehungskonfiguration für das interne Netzwerk hinzu. Auf diese Weise kann das System die Benutzeridentitätszuweisung für Anforderungen beibehalten, die von diesen Netzwerken ausgehen.

Schritt 3: Anwendungszugriff testen

Nach der Implementierung des IP-Ersatz-Dienstprogramms testen Sie die betroffenen Anwendungen, um sicherzustellen, dass:

- Domänenübergreifende Ressourcenanforderungen werden der Benutzeridentität ordnungsgemäß zugeordnet.
- Anwendungen ohne CORS-Fehler erfolgreich initialisiert

- Aktivitätsprotokolle zeigen für alle Anforderungen die Benutzeridentität statt der Netzwerk- oder Tunnelidentität an.

Schritt 5: Aktivitätsberichte überwachen

Verwenden Sie Monitor > Activity Search (Überwachung > Aktivitätssuche), um zu überprüfen, ob Anforderungen nun ordnungsgemäß authentifizierten Benutzern zugewiesen wurden, anstatt als netzwerk- oder tunnelbasierte Identität angezeigt zu werden.

Ursache

Dieses Verhalten wird aufgrund der Art der SAML-Authentifizierung in Verbindung mit Cookie Surrogate in virtualisierten Umgebungen erwartet. Wenn Webanwendungen domänenübergreifende Umleitungen durchführen oder Ressourcen von mehreren verwandten Domänen abrufen, enthalten die umgeleiteten Anfragen möglicherweise nicht das Surrogat-Cookie, sodass Cisco Secure Access eine Verbindung zur authentifizierten Benutzersitzung herstellen kann.

Die Ursache liegt in folgenden Gründen:

- Cookie Surrogate stützt sich auf Browser-Cookie-Übertragung über Umleitungen.
- Domänenübergreifende Sicherheitsrichtlinien (CORS) können Cookies in 307/Umleitungsszenarien entfernen.
- Browser-Sicherheitsmaßnahmen verhindern die gemeinsame Nutzung von Cookies über verschiedene Domänen hinweg.
- Virtuelle Desktop-Umgebungen behandeln die Verbreitung von Cookies anders als physische Systeme.

Sobald die Zuordnung zwischen Benutzern und Cookies verloren geht, kann Secure Access die Anforderung nicht an den authentifizierten Benutzer auflösen, sodass die Anforderung nur dem registrierten Netzwerk/der unterschiedlichen Identität als Quelle zugeordnet und anschließend durch standardmäßige Ablehnungsregeln blockiert wird.

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.