

SSL-Zertifikat- und Handshake-Fehler in sicherem Zugriff verstehen

Inhalt

Problem

Der aufgrund von Zertifikat- und TLS-Fehlern blockierte HTTP-Datenverkehr kann jetzt auf der Dashboard-Aktivitätssuche angezeigt werden. Dieser Artikel enthält eine Liste gängiger Fehlermeldungen sowie eine kurze Erläuterung der einzelnen Fehler.

Umwelt

- Cisco Secure Access - Secure Web Gateway SSL Inspection

Auflösung

Upstream-Zertifikat abgelaufen

Das Zertifikat der Website hat sein Ablaufdatum überschritten, daher vertraut Cisco Secure Access dem Zertifikat nicht. Diese ist auf der Website-Besitzer zu beheben, so erreichen Sie den Webmaster der Website und lassen Sie sie wissen.

Upstream-Zertifikat selbstsigniert

Die Website präsentiert ein Zertifikat, das sie selbst signiert hat, und kein Zertifikat, das von einer

vertrauenswürdigen Zertifizierungsstelle ausgestellt wurde. Da keine unabhängige Stelle dafür bürgt, kann Cisco Secure Access die Echtheit des Zertifikats nicht bestätigen.

Oft sehen Sie selbstsignierte Zertifikate auf Ressourcen, die für eine kleine, interne Zielgruppe bestimmt sind - die Admin-Portale auf IT-Sicherheits-Appliances sind ein klassisches Beispiel. Beachten Sie, dass Cisco Secure Access nicht so konfiguriert werden kann, dass selbstsignierte Zertifikate als vertrauenswürdig eingestuft werden.

Zwischenzertifikat fehlt

Cisco Secure Access konnte nicht alle benötigten Zwischenzertifikate sammeln und kann daher nicht die gesamte Vertrauenskette zu einem Stamm aufbauen.

Hier sind die Gründe, warum das wichtig ist: Das Zertifikat einer Website (das "Leaf") wird von einem Zwischenzertifikat signiert, das wiederum von einem anderen Zwischenzertifikat signiert werden kann, und so weiter bis zu einem vertrauenswürdigen Stamm. Damit diese Kette auschecken kann, muss die Website ihre Zwischenzertifikate zusammen mit ihren eigenen versenden. Wenn diese fehlen, bricht die Validierung zusammen - lassen Sie es den Webmaster der Website wissen.

Es gibt eine Ausnahme: Wenn das Zertifikat die Erweiterung "Authority Information Access" (AIA) enthält, kann Cisco Secure Access versuchen, die fehlenden Intermediate selbst abzurufen. Beachten Sie, dass dies nur funktioniert, wenn sowohl HTTPS-Entschlüsselung als auch Dateiinspektion aktiviert sind.

Upstream-Zertifikat fehlt der Antragstellername

Das Zertifikat enthält weder einen Antragstellernamen (einen Distinguished Name) noch einen alternativen Antragstellernamen, d. h. es gibt keine eindeutige Angabe, wem das Zertifikat gehört. Andernfalls kann Cisco Secure Access die Validierung nicht durchführen. Dies ist etwas, das der Website-Besitzer korrigieren muss.

Upstream-Zertifikat fehlt allgemeiner Name

Das Zertifikat hat keinen Common Name (CN) - das Feld, das traditionell den Hostnamen des

Standorts enthielt und bei der Bestätigung half, dass das Zertifikat tatsächlich zu dem Standort gehört, den Sie besuchen. Heutzutage hängt diese Prüfung wirklich vom alternativen Antragstellernamen (SAN) ab, und CN wird als Legacy-Feld betrachtet, aber das Fehlen dieses Felds kann diesen Fehler immer noch auslösen. Wenden Sie sich an den Webmaster, um es adressieren zu lassen.

Upstream-Zertifikat nicht vertrauenswürdig

Cisco Secure Access vertraut diesem Zertifikat nicht, in der Regel, weil es die ausstellende Root-Zertifizierungsstelle nicht erkennt.

Die Cisco Secure Access SWG führt eine integrierte Liste vertrauenswürdiger Stammzertifizierungsstellen, die von einem renommierten Anbieter bezogen und auf dem neuesten Stand gehalten werden. Wenn das Zertifikat eines Standorts zu einer Zertifizierungsstelle zurückverfolgt wird, die nicht in dieser Liste aufgeführt ist, schlägt die Validierung fehl. Wenn Sie sich sicher sind, dass die Root-Zertifizierungsstelle vertrauenswürdig ist, wenden Sie sich an den technischen Support. Wir werden uns umgehend mit Ihnen in Verbindung setzen.

Der Hostname im Zertifikat unterscheidet sich von dem erwarteten

Die von Ihnen angeforderte Adresse stimmt nicht mit dem Namen auf dem Zertifikat überein - weder mit dem Common Name (CN) noch mit einem alternativen Subjektnamen (SAN). Da das Zertifikat anscheinend nicht zu dem Standort gehört, den Sie erreichen, vertraut Cisco Secure Access ihm für diese Anforderung nicht. Der Webmaster muss das klären.

Upstream-Zertifikat widerrufen

Die Zertifizierungsstelle, die dieses Zertifikat ausgestellt hat, hat es inzwischen widerrufen, d. h. es gilt nicht mehr als gültig.

Cisco Secure Access bestätigt dies mithilfe des Online Certificate Status Protocol (OCSP), das in Echtzeit überprüft, ob ein Zertifikat widerrufen wurde. Lassen Sie den Webmaster der Website wissen, damit sie es ersetzen können.

TLS-Handshake-Fehler

Nicht unterstützte Upstream-Verschlüsselung

Der TLS-Handshake konnte nicht abgeschlossen werden, da die Website keine der von der Cisco Secure Access SWG verwendeten Verschlüsselungssuiten unterstützt. Dies zeigt sich häufig bei älteren oder veralteten Servern, die nur schwächere Chiffren anbieten. Das Fix liegt auf der Serverseite, also gib es an den Webmaster weiter.

Upstream-TLS-Versionskonflikt

Der Handshake schlug fehl, da die Website keine TLS-Version verwendet, die von der Cisco Secure Access SWG unterstützt wird. Der Cisco Secure Access SWG-Proxy arbeitet derzeit mit TLS 1.2 und TLS 1.3 zusammen - sowohl für Verbindungen, die von Clients eingehen, als auch für Verbindungen, die er zu Zielserversn herstellt.

Upstream-DH-Schlüssel kleiner als 1024 Bit

Der Handshake konnte nicht abgeschlossen werden, da die Website einen Diffie-Hellman-Schlüssel verwendet, der zu schwach (unter 1024 Bit) ist, als dass Cisco Secure Access ihn akzeptieren könnte. Dies ist eine serverseitige Einschränkung, sodass der Webmaster es verstärken muss.

Problemumgehungen

Sie können diese Probleme umgehen, indem Sie Konfigurationsänderungen in Cisco Secure Access vornehmen.

Dies muss nur geschehen, wenn Sie der Authentizität des Servers und des Zertifikats vertrauen.

Workarounds können mithilfe eines Eintrags in der "Selektiven Entschlüsselungsliste" (Selective

Decryption List) zur Deaktivierung der Entschlüsselung oder eines Eintrags in der Rubrik "Externe Domänen" (External Domains) zur vollständigen Umgehung des Datenverkehrs von Cisco Secure Access angewendet werden. Wenn die Entschlüsselung deaktiviert ist, führt der Cisco Secure Access keine Zertifikatvalidierung durch.

Beachten Sie, dass der Browser in den meisten Fällen immer noch einen Fehler oder eine Warnung anzeigt, wenn der Datenverkehr von Cisco Secure Access umgangen wird. Webbrowser führen eine ähnliche Zertifikatsvalidierung durch.

Ursache

Der TLS-Handshake konnte vom Cisco Secure Access SSL-Überprüfungsproxy nicht abgeschlossen werden - in der Regel, weil das Ziel eine Zertifikatspin verwendet, die das neu signierte CSA-Zertifikat zurückweist.

- Zertifikat-Pinning: Client-Hartcodes erwarten Fingerabdruck für Zertifikat
- CSA CA auf Endgerät nicht vertrauenswürdig: Prüfungs-Zertifizierungsstellenzertifikat nicht im vertrauenswürdigen Stammspeicher bereitgestellt

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.