ASA Clientless-SSL-VPN: RDP-Plug-in-Probleme

Inhalt

Einführung

Dieses Dokument enthält Antworten auf einige häufig gestellte Fragen zum Remote Desktop Protocol (RDP)-Plug-in, das Benutzern von Cisco Adaptive Security Appliance (ASA) Clientless Secure Sockets Layer VPN (SSLVPN) zur Verfügung steht.

Das RDP-Plug-in ist neben anderen Plug-Ins wie Secure Shell (SSH), Virtual Network Computing (VNC) und Citrix nur eines der Plug-Ins, die Benutzern zur Verfügung stehen. Das RDP-Plug-in ist eines der am häufigsten verwendeten Plug-Ins in dieser Sammlung. Dieses Dokument enthält weitere Details zur Bereitstellung und Fehlerbehebung für dieses Plug-in.

> **Hinweis**: Dieses Dokument enthält keine Informationen zur Konfiguration des RDP-Plug-ins. Weitere Informationen finden Sie im Cisco ASA 5500 SSL VPN Deployment Guide, Version 8.x.

Hintergrundinformationen

Das RDP-Plug-in wurde von einem reinen Java-basierten RDP-Plug-in entwickelt und umfasst sowohl den ActiveX RDP-Client (Internet Explorer) als auch den Java-Client (Browser, die nicht zum Internet Explorer gehören).

Java-Plug-In

Der Java RDP Client verwendet das richtige Java RDP-Applet. Das Java-Applet wird dann in ein Plug-in eingeschlossen, das die Installation im clientlosen ASA-Portal ermöglicht.

Active-X-Plug-In

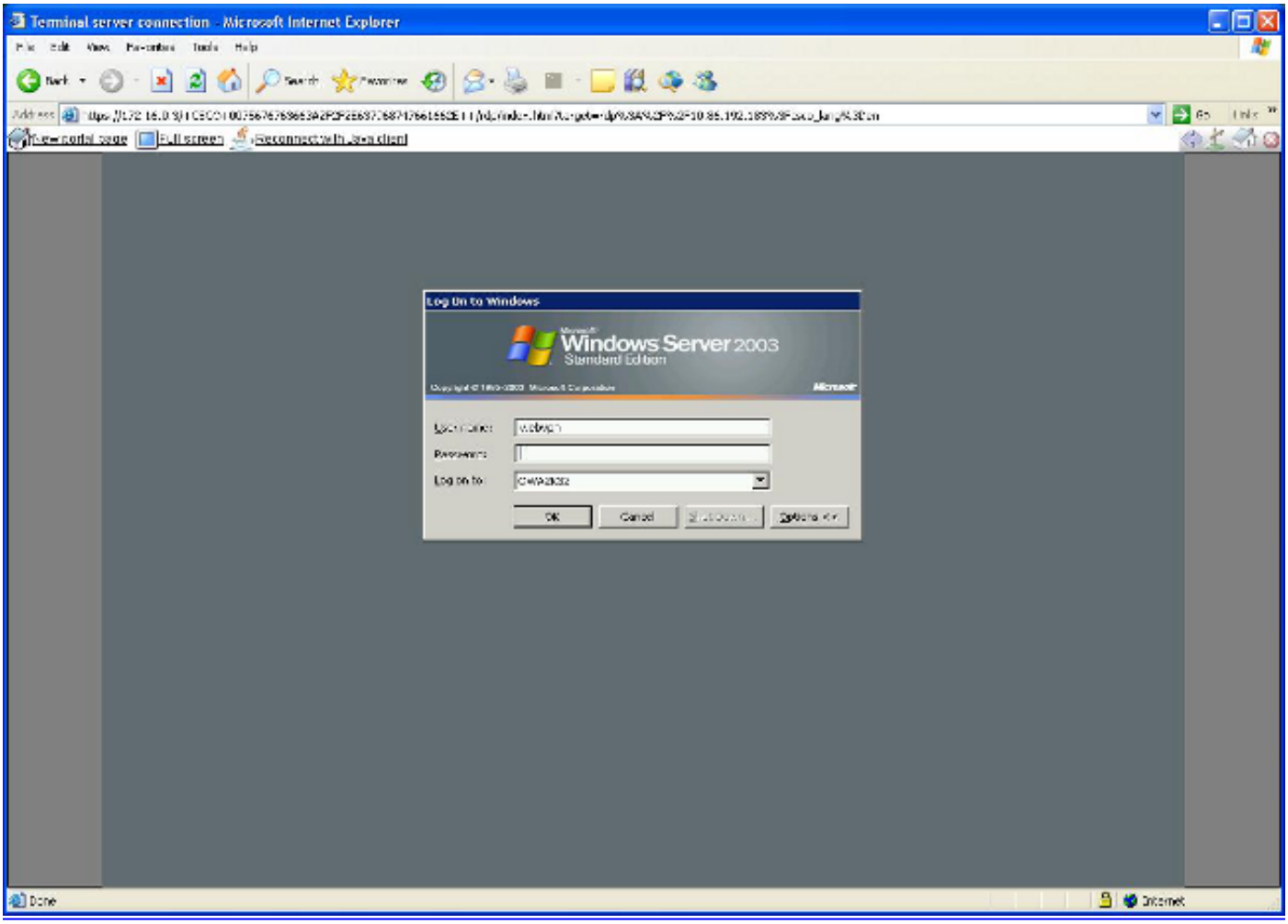
Das RDP-Plug-in beinhaltet auch den Microsoft ActiveX RDP Client, und das Plug-in bestimmt, ob Java oder ActiveX Client auf Basis des Browsers verwendet werden soll. Das heißt:

- Wenn Internet Explorer (IE)-Benutzer versuchen, RDP über ein Clientless-SSL-VPN-Portal zu verwenden, und die Lesezeichen-URL das **ForceJava=true-**Argument nicht enthält, wird der ActiveX-Client verwendet. Wenn ActiveX nicht ausgeführt werden kann, initiiert das Plug-in den Java-Client.
- Wenn Nicht-IE-Benutzer versuchen, ein RDP-Lesezeichen oder eine URL zu starten, wird nur der Java-Client gestartet.

Weitere Informationen zu Anforderungen für RDP-ActiveX- und USER-Berechtigungen finden Sie im Artikel Anforderungen von Microsoft für Remotedesktop-Webverbindung.

Das nächste Bild zeigt die drei Links, die im Browserfenster nach dem Starten des Plug-ins ausgewählt werden können:

1. **Neue Portalseite** - Über diesen Link wird die Portalseite in einem neuen Browserfenster geöffnet.
2. **Vollbildmodus** - Hiermit wird das RDP-Fenster im Vollbildmodus verwendet.
3. **Java erneut verbinden** - Dadurch wird das Plug-in gezwungen, erneut eine Verbindung herzustellen und Java anstelle von ActiveX zu verwenden.



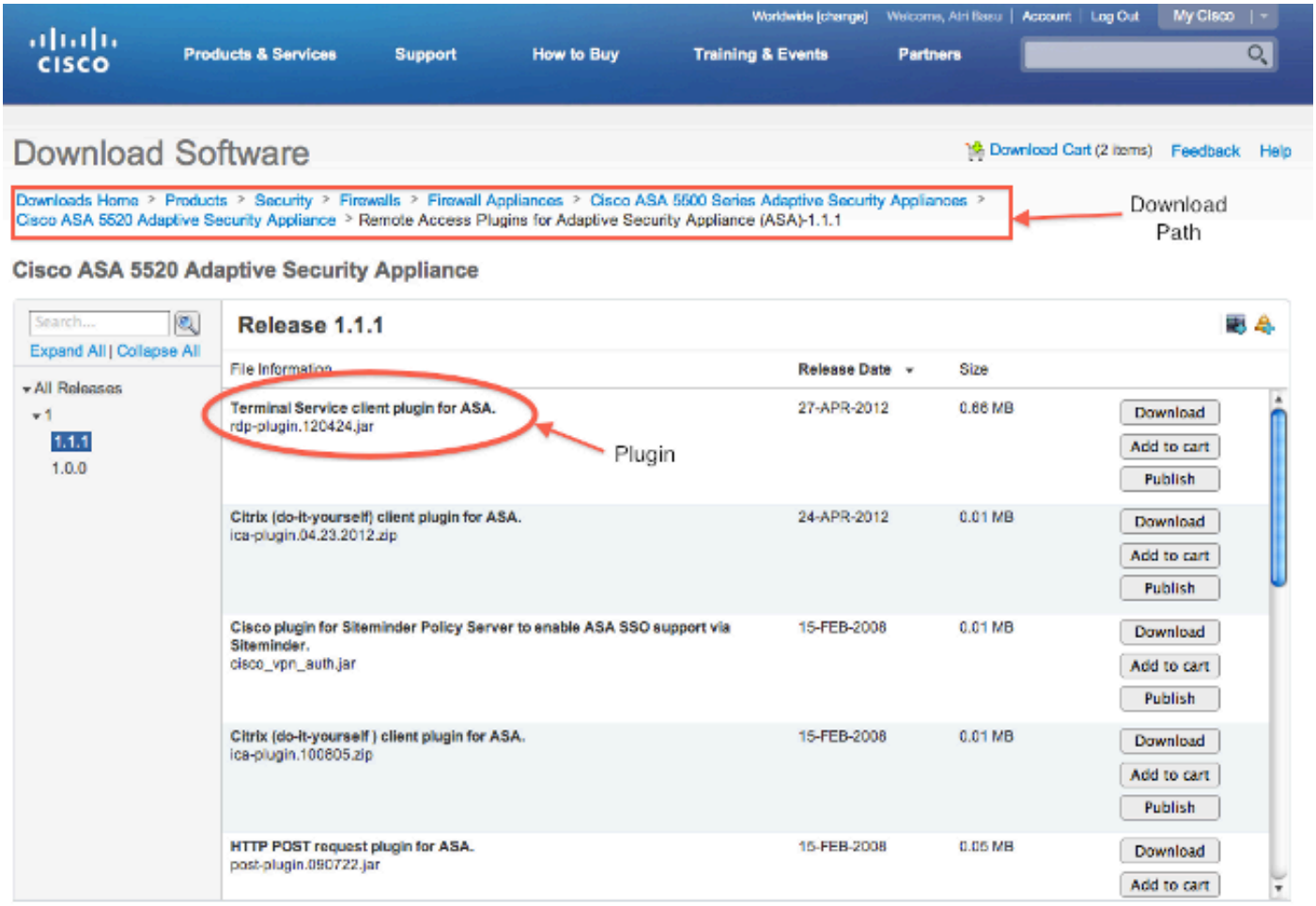
RDP-Plug-In

RDP- und RDP-2-Plug-In-Nutzung

- **RDP-Plug-in:** Dies ist das ursprüngliche Plug-In, das sowohl den Java- als auch den ActiveX-Client enthält.
- **RDP2-Plug-in:** Aufgrund von Änderungen im RDP-Protokoll wurde der richtige Java-RDP-Client aktualisiert, um Microsoft Windows 2003 Terminal-Server und Windows Vista Terminal-Server zu unterstützen.

  Tipp: Das neueste RDP-Plug-in kombiniert RDP- und RDP2-Protokolle. Infolgedessen ist das RDP2 Plug-in veraltet. Es wird empfohlen, die neueste Version des RDP-Plug-ins zu verwenden. Die RDP-Plug-in-Nomenklaturen folgen dieser Struktur: **rdp-plugin.ymmdd.jar**, wobei **yy** ein zweistelliges Jahresformat ist, **mm** ein zweistelliges Monatsformat und **dd** ein zweistelliges Tagformat.

Um das Plug-in herunterzuladen, besuchen Sie die Cisco Software Download-Seite.



Positionierung von ActiveX und Java-Clients im Vergleich

RDP-ActiveX

- Nur IE
- Unterstützung für weitergeleiteten Sound

RDP-Java

- Funktioniert auf allen unterstützten Browsern, die Java-fähig sind.
- Der Java-Client wird in IE nur dann gestartet, wenn ActiveX nicht gestartet werden kann, oder das Argument **ForceJava=true** wird im RDP-Lesezeichen übergeben.
- Die RDP-Java-Implementierung basiert auf einem geeigneten Java-RDP-Projekt, einer Open-Source-Initiative. Für die Anwendung wird bestmöglicher Support angeboten.

RDP-Bookmark-Format

Das folgende Beispiel zeigt ein RDP-Lesezeichen:

```
rdp://server:port/?Parameter1=value&Parameter2=value&Parameter3=value
```

Hier einige wichtige Hinweise zum Format:

- **server** - Dies ist das einzige erforderliche Attribut. Geben Sie den Namen des Computers ein, der die Microsoft Terminal Services hostet.
- **port** (optional) - Dies ist die virtuelle Adresse innerhalb des Remote-Computers, der die Microsoft Terminal Services hostet. Der Standardwert 3389 stimmt mit der bekannten Portnummer für Microsoft Terminal Services überein.
- **parameters** - Dies ist eine optionale Abfragezeichenfolge, die aus Parameterwert-Paaren besteht. Ein Fragezeichen demarkiert den Anfang der Argumentzeichenfolge, und jedes Parameterwertpaar wird durch einen Ampersand getrennt.

  Im Folgenden finden Sie eine Liste der verfügbaren Parameter:

  Geometrie - Dies ist die Größe des Client-Bildschirms in Pixel (W x H).**bpp**: Dies sind die Bits pro Pixel (Farbtiefe), 8|16|24|32.**Domäne**: Dies ist die Anmeldungsdomäne.**username** - Dies ist der Benutzername für die Anmeldung.**password** - Dies ist das Anmeldekennwort. Verwenden Sie das Passwort mit Vorsicht, da es auf der Client-Seite verwendet wird und beobachtet werden kann.**console** - Dies wird verwendet, um eine Verbindung zur Konsolensitzung auf dem Server herzustellen (Ja/Nein).**ForceJava** - Legen Sie diesen Parameter auf **yes** fest, um nur den Java-Client zu verwenden. Die Standardeinstellung ist **Nein**.**shell** - Legen Sie diesen Parameter auf den Pfad der ausführbaren Datei bzw. Anwendung fest, die automatisch gestartet wird, wenn Sie eine Verbindung mit RDP herstellen (**rdp://server/?shell=path**, z. B.).

  Im Folgenden finden Sie eine Liste zusätzlicher Parameter, die nur für ActiveX verwendet werden:

  RedirectDrives - Legen Sie diesen Parameter auf **true fest**, um Remote-Laufwerke lokal zuzuordnen.**RedirectPrinters** (**UmleitenDrucker**): Legen Sie diesen Parameter auf **true fest**, um Remote-Drucker lokal zuzuordnen.**Vollbild** - Legen Sie diesen Parameter auf **true fest**, um im Vollbildmodus zu starten.**ForceJava** - Legen Sie diesen Parameter auf **yes** fest, um den Java-Client zu erzwingen.**audio** - Dieser Parameter wird für die Audioweiterleitung über die RDP-Sitzung verwendet:

  0 - Leitet Remote-Sounds auf den Client-Computer um.**1** - Spielt Töne am Remote-Computer ab.**2** - Deaktiviert die Tonumleitung; ertönt keine Sounds auf dem Remote-Server.

RDP-Plug-In und VPN-Lastenausgleich

Der geografische Lastenausgleich wird durch den globalen Server-Lastenausgleich auf DNS-Basis (Domain Name Server) unterstützt. Aufgrund der Unterschiede bei der DNS-Ergebniszwischenspeicherung können Plug-Ins auf verschiedenen Betriebssystemen unterschiedlich funktionieren. Mit dem Windows DNS-Cache kann das Plug-in dieselbe IP-Adresse auflösen, wenn es das Java-Applet startet. Auf Macintosh (MAC) OS X kann das Java-Applet eine andere IP-Adresse auflösen. Daher kann das Plug-in nicht ordnungsgemäß gestartet werden.

Ein Beispiel für DNS Round-Robin ist, wenn Sie eine einzige URL (https://www.example.com) haben, über die der DNS-Eintrag für **www.example.com** entweder 192.0.2.10 (ASA1) oder

198.51.100.50 (ASA2) auflösen kann.

Nachdem sich der Benutzer über einen Browser auf ASA1 beim Clientless-WebVPN-Portal angemeldet hat, ist die Initiierung des RDP-Plug-ins möglich. Während der Initiierung des Java-Clients führen MAC OS X-Computer eine neue DNS-Auflösungsanfrage aus. Bei einer Round-Robin-DNS-Konfiguration besteht eine Wahrscheinlichkeit von 50 %, dass diese zweite Auflösungsantwort dieselbe Website zurückgibt, die für die erste WebVPN-Verbindung gewählt wurde. Wenn die Antwort des DNS-Servers 198.51.100.50 (ASA2) und nicht 192.0.2.10 (ASA1) lautet, initiiert der Java-Client eine Verbindung zur falschen ASA (ASA2). Da die Benutzersitzung auf der ASA2 nicht vorhanden ist, wird die Verbindungsanforderung abgelehnt.

Dies kann Java-Fehlermeldungen ähnlich der folgenden ergeben:

```
java.lang.ClassFormatError: Incompatible magic value 1008813135 in
 class file net/propero/rdp/applet/RdpApplet
```

Häufig gestellte Fragen

Warum erscheinen einige typisierte Zeichen nicht in der Remote-RDP-Sitzung?

Der Remote-Computer in der RDP-Sitzung kann eine andere Einstellung für den Tastaturbereich haben als der lokale Computer. Aufgrund dieser Unterschiede werden auf dem Remote-Computer möglicherweise keine bestimmten typisierten Zeichen oder falschen Zeichen angezeigt. Dieses Verhalten wird nur mit dem Java-Plug-in beobachtet. Um dieses Problem zu beheben, verwenden Sie das **keymap-**Attribut, um die lokale Tastatur dem Remote-PC zuzuordnen.

Um beispielsweise eine deutsche Tastaturzuordnung festzulegen, verwenden Sie:

```
rdp://
```

```
The following keymaps are available:
----------------------------------------------------------------------
ar    de    en-us fi    fr-be it    lt    mk    pl    pt-br sl    tk
da    en-gb es    fr    hr    ja    lv    no    pt    ru    sv    tr
----------------------------------------------------------------------
```

Bekannte Probleme mit Tastaturzuordnungen

- Cisco Bug ID CSCth38454 - **Implementieren der ungarischen Tastatur für das RDP-Plug-in.**
- Cisco Bug-ID CSCsu77600 - **Die Bildschirmtasten des WebVPN RDP-Plugins sind falsch. Umschalttaste (Taste) .jar**.
- Cisco Bug-ID CSCtt04614 - **WebVPN - ES-Tastaturdiakritiken, die nicht korrekt über das RDP-Plugin verwaltet werden.**

- Cisco Bug-ID CSCtb07767 - **ASA Plugin - Konfigurieren Sie die Standardparameter**.

  Tipp: Eine weitere mögliche Problemumgehung ist die Verwendung eines Application Smart Tunnel für **mstsc.exe.** Dies wird im WebVPN-Unterkonfigurationsmodus mit dem folgenden Befehl konfiguriert: **Plattformfenster für die Smart-Tunnel-Liste RDP_List RDP mstsc.exe**.

Kann das Java RDP-Plug-in RDP-Sitzungen im Vollbildmodus unterstützen?

Derzeit werden RDP-Sitzungen im Vollbildmodus nicht nativ unterstützt. Die CSCto87451-Verbesserungsanfrage wurde eingereicht, um dies zu implementieren. Wenn der **Geometrieparameter** (**Geometrie = 1024x768** zum Beispiel) auf die Auflösung des Benutzerbildschirms eingestellt ist, arbeitet er im Vollbildmodus. Da die Größe des Benutzerbildschirms variiert, kann es erforderlich sein, mehrere Lesezeichen-Links zu erstellen. Der ActiveX-Client unterstützt nativ Vollbild-RDP-Sitzungen.

Kann der Java-Client mit AES-256 für Verschlüsselung kommunizieren?

Damit der Java-Client das SSL korrekt aushandeln kann, passen Sie die Reihenfolge des ASA SSL-Verschlüsselungssatzes an die folgende Reihenfolge an:

```
Enabled cipher order: aes256-sha1 rc4-sha1 aes128-sha1 3des-sha1
Disabled ciphers: des-sha1 rc4-md5 null-sha1
```

Der Java-Client kann diesen Fehler anzeigen, wenn die Reihenfolge der Verschlüsselung anders ist:

```
[Thread-12] INFO net.propero.rdp.Rdp - javax.net.ssl.SSLHandshakeException:
 Received fatal alert: handshake_failure
```

RDP-Probleme beheben

Wenn Sie andere Probleme mit dem RDP-Plug-In haben, können Sie diese Daten möglicherweise sammeln, um RDP-Probleme zu beheben:

- Die **Show-Tech-**Ausgabe der ASA
- Das **show import webvpn-Plug-in zeigt detaillierte** Ausgabe von der ASA
- Betriebssystem des Benutzercomputers und Patch-Level
- Das Betriebssystem des Zielcomputers und die Patch-Level
- Der verwendete Client (ActiveX- oder Java-Version) und Java JRE-Version
- Bestimmen Sie, ob sich die ASA in einem Cluster, DNS-basiert oder ASA-basiert mit Lastenausgleich befindet.

Bekannte Einwände

Probleme mit Microsoft Security Update

1. KB2695962 - Microsoft Security Advisory: Update-Rollup für ActiveX-Kill-Bits: 8. Mai 2012.
2. KB2675157 - MS12-023: Kumulative Sicherheits-Update für Internet Explorer: 10. April 2012.
3. cisco-sa-20120314-asaclient - Clientless VPN ActiveX Control Remote Code Execution Schwachstelle der Cisco Adaptive Security Appliance der Serie ASA 5500 - 14. März.
4. Cisco Bug ID CSCtx68075 - ASA WebVPN Break, wenn Windows Patch KB2585542 angewendet wird (8.2.5.29 / 8.4.3.9).
5. KB2585542 - MS12-006: Beschreibung des Sicherheitsupdates für Webio, Winhttp und Game in Windows: 10. Januar 2012.

ActiveX-Client

- **Symptome**: Der ActiveX-Client kann nach einem Upgrade auf die ASA-Betriebssystemversion 8.4.3 nicht von IE 6 bis 9 geladen werden.

  Weitere Informationen finden Sie unter Cisco Bug ID CSCtx58556. Die Reparatur ist ab Version 8.4.3.4 verfügbar.Problemumgehung: Erzwingen Sie die Verwendung des Java-Clients.

- **Symptome**: Der ActiveX-Client kann nicht geladen werden, nachdem die ASA-Betriebssystemversion auf eine Version vor 8.4.3 herabgestuft wurde. Dies betrifft Benutzer, die den ActiveX-Client auf einem ASA-Gerät mit der Behebung für die Cisco Bug-ID CSCtx58556 verwendet haben und mit einer Version vor 8.4.3 eine Verbindung zu dieser ASA herstellen. Dies liegt an einem neuen ActiveX RDP-Plug-in in ASA Version 8.4.3, das nicht mit den früheren Versionen kompatibel ist.

  Weitere Informationen finden Sie unter Cisco Bug ID CSCtx57453.Entfernen Sie alle Windows-Registrierungsinstanzen von **b8e73359-3422-4384-8d27-4ea1b4c01232?** (alte ActiveX-CLSID).

  Hinweis: Es wird empfohlen, vor allen Änderungen eine Sicherung der Computersystemregistrierung durchzuführen.
- **Symptome**: RDP-Verbindungen zu Geräten mit aktivierter Network Level Authentication (NLA) schlagen fehl.

  Die Erweiterung, bei der NLA in das ActiveX-RDP-Plug-In integriert werden soll, wird unter CSCtu63661 der Cisco Bug-ID angefordert.Obwohl Microsoft ActiveX-Client NLA unterstützt, wird die Verwendung dieser Funktion innerhalb des ASA-Plug-ins nicht unterstützt.Problemumgehung: Konfigurieren Sie das RDP-Plug-In (**mstsc.exe**) für den Smart-Tunneling. Weitere Informationen finden Sie im Cisco ASA 5500 SSL VPN Deployment Guide, Version 8.x.

- **Symptome**: ActiveX-RDP wird nicht geladen, und es wird eine leere Seite angezeigt.

  Weitere Informationen finden Sie unter Cisco Bug ID CSCsx49794.Dies tritt auf, wenn die Zertifikatskette für das ASA SSL-Zertifikat größer als vier Zertifikate ist (z. B. ROOT, SUBCA1, SUBCA2 und ASA CERT).Problemumgehung:

Installieren Sie nicht die große Zertifikatskette auf der ASA.Im Gegensatz zum ActiveX-Plug-in ist bekannt, dass das Java-RDP-Plug-In ordnungsgemäß funktioniert.RDP funktioniert auch ordnungsgemäß, wenn Sie systemeigene Windows **mstsc.exe** mit Smart Tunnels konfigurieren.

- **Symptome**: Nachdem der ActiveX-RDP-Client verwendet wurde, klickt ein Benutzer auf die **Logout-**Schaltfläche und erhält einen **HTTP 404 - Page Not found-**Fehler. Weitere Informationen finden Sie unter Cisco Bug ID CSCtz33266. Dieses Problem wurde mit der Plug-in-Version **rdp-plugin.120424.jar** oder höher behoben.

- **Symptome**: Ein Benutzer hat im IE zwei Registerkarten geöffnet - eine für die RDP-Sitzung und eine andere für eine leere oder andere Webseite. IE funktioniert nach Schließen der RDP-Registerkarte nicht ordnungsgemäß.

  Weitere Informationen finden Sie unter Cisco Bug ID CSCua69129.Problemumgehung: Verwenden Sie das Java RDP-Plug-in (Set **ForceJava=true**).

- **Symptome**: Das ActiveX-Plug-in verursacht eine hohe CPU-Auslastung bei IE. Weitere Informationen finden Sie unter Cisco Bug ID CSCua16597.

- **Symptome**: Nach der Installation von Windows Update **KB2695962** wird das ActiveX RDP-Plug-In nicht geladen. Wenn eine neue RDP-Sitzung geöffnet wird, versucht der ActiveX-Client, den **Cisco SSL VPN Port Forwarder** zu installieren (dies geschieht nicht immer) und kehrt zur clientlosen Portalseite zurück, ohne eine Verbindung zum Remote-Computer herzustellen. Dies ist auf die Schwachstelle **CVE-2012-0358** zurückzuführen**,** die clientseitig durch Microsoft Security Advisory (2695962) behoben wird.

  Weitere Informationen finden Sie in Cisco Security Advisory Cisco Adaptive Security Appliance der Serie ASA 5500 Clientless VPN ActiveX Control Remote Code Execution Vulnerability.Weitere Informationen finden Sie unter Cisco Bug ID CSCtr00165.

Java-Client

Hinweis: Cisco verteilt Plug-Ins ohne Änderungen neu. Aufgrund der GNU General Public License ändert oder erweitert Cisco die Plug-in-Anwendung nicht. Das **korrekte JavaRDP**-Plug-In ist eine Open-Source-Anwendung, und alle Probleme mit der Plug-In-Software müssen vom Projekteigentümer behoben werden.

- **Symptome**: Auf dem Remote-Computer werden prozessorintensive Anwendungen ausgeführt, wenn der Zugriff über den Java-RDP-Client erfolgt, und es kommt zu einem Absturz des Java-Applets.

  Diese Fehlermeldung kann angezeigt werden: **FATAL net.properties.rdp - javax.net.ssl.SSLException: Die Verbindung wurde heruntergefahren: ....**.Das Verhalten wird ausgelöst, wenn schnell zwischen zwei oder mehr CPU-intensiven Anwendungen umgeschaltet wird.Dieses Problem wurde in den Plug-in-Versionen rdp.2012.6.4.jar und höher behoben. Problemumgehung:

Stellen Sie eine Verbindung mit der Verwendung des ActiveX-Clients her.Wechseln Sie nicht schnell zwischen Anwendungen.

- **Symptome**: Der Java RDP-Client generiert die folgende Fehlermeldung: **net.properties.rdp.Rdp - java.net.SocketException: Socket wird geschlossen java.net.SocketException: Der Sockel wird geschlossen** und dann geschlossen.

  Das Problem wird durch eine Tunnelgruppe verursacht, für die eine group-url nur mit dem FQDN konfiguriert ist (z. B. http://www.example.com).Weitere Informationen finden Sie unter Cisco Bug ID CSCuh72888.Problemumgehung:

  Entfernen Sie den Gruppen-URL-Eintrag ohne "/" in der Tunnelgruppe.Verwenden Sie den ActiveX-Client.

- **Symptome**: Der Java RDP-Client schlägt fehl, wenn er an einen Windows 8-Computer angeschlossen ist.

  Der Java RDP Client unterstützt dies derzeit nicht.Siehe Cisco Bug-ID CSCuc79990Problemumgehung:

  Verwenden Sie den ActiveX RDP-Client.Intelligenter Tunnel zum nativen RDP-Client von Windows (**mstsc.exe**)

- **Symptome**: Der Java RDP-Client schlägt mit der folgenden Fehlermeldung fehl: **ARSigningException: Nicht signierter Eintrag in Ressource gefunden: https://10.105.130.91/+CSCO+3a75676763663A2F2F2E637968747661662E++/vnc/VncViewer.jar**.

  Dieses Problem wird durch einen Fehler in der ASA WebVPN Java Rewriter verursacht.Weitere Informationen finden Sie unter Cisco Bug ID CSCuj88114.Problemumgehung: Downgrade auf Java Version 7u40.