SSLVPN senza client ASA: Problemi dei plug-in RDP

Sommario

Introduzione

In questo documento vengono fornite le risposte ad alcune domande frequenti sul plug-in RDP (Remote Desktop Protocol), disponibile per gli utenti di Cisco Adaptive Security Appliance (ASA) Secure Sockets Layer VPN (SSLVPN) senza client.

Il plug-in RDP è solo uno dei plug-in disponibili per gli utenti, insieme ad altri come Secure Shell (SSH), Virtual Network Computing (VNC) e Citrix. Il plug-in RDP è uno dei plug-in utilizzati più di frequente in questa raccolta. In questo documento vengono fornite informazioni dettagliate sulla distribuzione e sulle procedure di risoluzione dei problemi per questo plug-in.

> **Nota:** In questo documento non vengono fornite informazioni su come configurare il plug-in RDP. Per ulteriori informazioni, consultare la guida all'implementazione di Cisco ASA 5500 SSL VPN, versione 8.x.

Premesse

Il plug-in RDP è stato sviluppato da un plug-in RDP basato esclusivamente su Java, per includere sia il client ActiveX RDP (Internet Explorer) che il client Java (browser non Internet Explorer).

Plug-in Java

Il client Java RDP utilizza l'applet Java RDP appropriata. L'applet Java viene quindi incapsulata in un plug-in che consente l'installazione all'interno del portale senza client ASA.

Plug-in Active-X

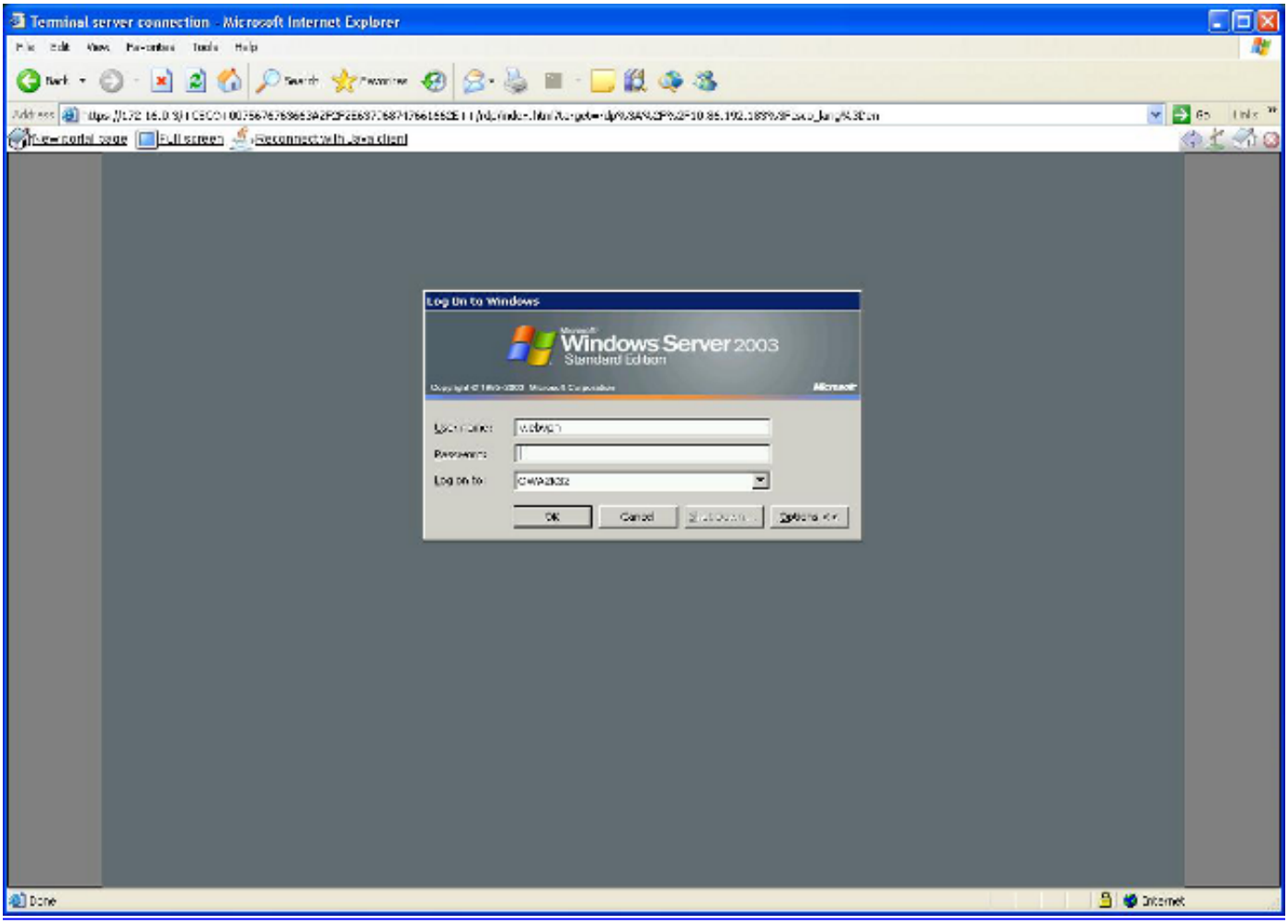
Il plug-in RDP include inoltre il client RDP Microsoft ActiveX e determina se utilizzare Java o il client ActiveX in base al browser. Cioè:

- Se gli utenti di Internet Explorer (IE) tentano di utilizzare RDP tramite un portale SSLVPN senza client e l'URL del segnalibro non contiene l'argomento **ForceJava=true**, viene utilizzato il client ActiveX. Se l'esecuzione di ActiveX non riesce, il plug-in avvia il client Java.
- Se utenti non IE tentano di avviare un segnalibro RDP o un URL, viene avviato solo il client Java.

Per ulteriori informazioni sui requisiti per i privilegi RDP ActiveX e USER, fare riferimento all'articolo Requisiti di Microsoft per Connessione Web desktop remoto.

L'immagine seguente mostra i tre collegamenti che è possibile selezionare nella finestra del browser dopo l'avvio del plug-in:

1. **Nuova pagina portale** - Questo collegamento consente di aprire la pagina del portale in una nuova finestra del browser.
2. **Schermo intero** - Viene utilizzata la finestra RDP in modalità a schermo intero.
3. **Riconnetti con Java** - Impone al plug-in di riconnettersi e utilizzare Java anziché ActiveX.



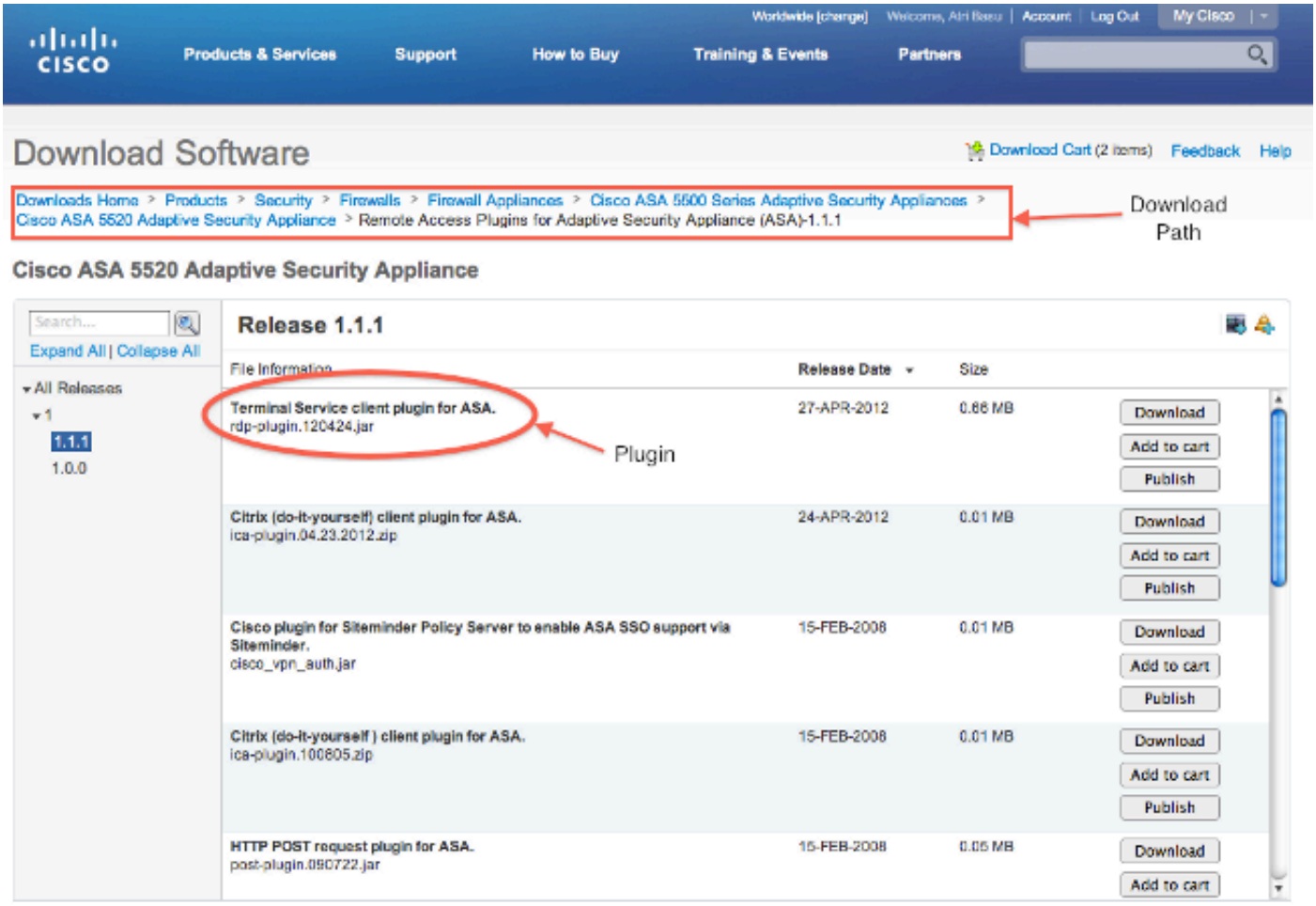
Plug-in RDP

Utilizzo dei plug-in RDP e RDP-2

- **Plug-in RDP:** si tratta del plug-in originale creato che contiene sia Java che ActiveX Client.
- **Plug-in RDP2:** a causa di modifiche apportate al protocollo RDP, il client RDP Java appropriato è stato aggiornato per supportare i Terminal Server di Microsoft Windows 2003 e Windows Vista.

  Suggerimento: Il plug-in RDP più recente combina i protocolli RDP e RDP2. Di conseguenza, il plug-in RDP2 è obsoleto. Si consiglia di utilizzare la versione più recente del plug-in RDP. Le nomenclature plug-in RDP seguono questa struttura: **rdp-plugin.yymmdd.jar**, dove **yy** è un formato anno a due cifre, **mm** è un formato mese a due cifre e **dd** è un formato giorno a due cifre.

Per scaricare il plug-in, visitare la pagina di download del software Cisco.



Posizionamento dei client ActiveX e Java

RDP-ActiveX

- Utilizza solo IE
- Fornisce supporto per l'audio inoltrato

RDP-Java

- Funziona su tutti i browser supportati abilitati per Java.
- Il client Java viene avviato in IE solo se l'avvio di ActiveX non riesce o se l'argomento **ForceJava=true** passa nel segnalibro RDP.
- L'implementazione di RDP-Java si basa su un progetto RDP Java appropriato, un'iniziativa open-source; per l'applicazione viene fornito il supporto più efficiente.

Formato segnalibro RDP

Di seguito è riportato un esempio di formato di un segnalibro RDP:

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

Ecco alcune note importanti sul formato:

- **server** - Questo è l'unico attributo obbligatorio. Immettere il nome del computer che ospita Servizi terminal Microsoft.
- **porta** (facoltativo): indirizzo virtuale del computer remoto che ospita Servizi terminal Microsoft. Il valore predefinito, 3389, corrisponde al numero di porta conosciuto per Servizi terminal Microsoft.
- **parameters** - Stringa di query facoltativa costituita da coppie parametro-valore. Un punto interrogativo indica l'inizio della stringa dell'argomento e ogni coppia parametro-valore è separata da una e commerciale.

  Di seguito è riportato un elenco dei parametri disponibili:

  Geometria: dimensioni dello schermo client in pixel (L x A).**bpp** - Bit per pixel (profondità colore), 8|16|24|32.**domain** - Dominio di accesso.**username** - Nome utente per l'accesso.**password** - Password di accesso. Utilizzare la password con cautela, in quanto viene utilizzata sul lato client ed è osservabile.**console** - Questa opzione viene utilizzata per connettersi alla sessione console sul server (sì/no).**ForceJava** - Impostare questo parametro su **yes** per utilizzare solo il client Java. L'impostazione predefinita è **no**.**shell**: impostare questo parametro sul percorso dell'eseguibile/applicazione che viene avviato automaticamente quando ci si connette a RDP (ad esempio, **rdp://server/?shell=path**).

  Di seguito è riportato un elenco di parametri aggiuntivi solo ActiveX:

  RedirectDrives: impostare questo parametro su **true** per mappare le unità remote localmente.**RedirectPrinters**: impostare questo parametro su **true** per mappare le stampanti remote localmente.**FullScreen**: impostare questo parametro su **true** per l'avvio in modalità FullScreen.**ForceJava** - Impostare questo parametro su **yes** per forzare il client Java.**audio**: questo parametro viene utilizzato per l'inoltro audio nella sessione RDP:

  0 - Reindirizza i suoni remoti al computer client.**1** - Riproduce l'audio sul computer remoto.**2** - Disattiva il reindirizzamento audio; non riproduce suoni sul server remoto.

Plug-in RDP e bilanciamento del carico VPN

Il bilanciamento del carico su più aree geografiche è supportato con l'utilizzo del bilanciamento del carico del server globale basato su DNS (Domain Name Server). A causa delle differenze nella cache dei risultati DNS, i plug-in potrebbero funzionare in modo diverso nei diversi sistemi operativi. La cache DNS di Windows consente al plug-in di risolvere lo stesso indirizzo IP quando avvia l'applet Java. In Macintosh (MAC) OS X, è possibile che l'applet Java risolva un indirizzo IP diverso. Di conseguenza, il plug-in non viene avviato correttamente.

Un esempio di round-robin DNS si ha quando si ha un singolo URL (https://www.example.com) in cui la voce DNS per **www.example.com** può risolvere 192.0.2.10 (ASA1) o 198.51.100.50 (ASA2).

Dopo aver effettuato l'accesso al portale WebVPN senza client tramite un browser su ASA1, è possibile avviare il plug-in RDP. Durante l'avvio del client Java, i computer MAC OS X eseguono una nuova richiesta di risoluzione DNS. Con una configurazione DNS round-robin, esiste il 50% di possibilità che questa seconda risposta di risoluzione restituisca lo stesso sito scelto per la

connessione WebVPN iniziale. Se la risposta del server DNS è 198.51.100.50 (ASA2) anziché 192.0.2.10 (ASA1), il client Java avvia una connessione all'ASA errata (ASA2). Poiché la sessione utente non esiste sull'appliance ASA2, la richiesta di connessione viene rifiutata.

Ciò potrebbe causare messaggi di errore Java simili al seguente:

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

Wireless LAN Controller serie 9800

Perché alcuni caratteri digitati non vengono visualizzati nella sessione RDP remota?

Èpossibile che nel computer remoto della sessione RDP sia impostata un'area della tastiera diversa da quella del computer locale. A causa di questa differenza, è possibile che nel computer remoto non vengano visualizzati determinati caratteri digitati o non corretti. Questo comportamento viene rilevato solo con il plug-in Java. Per risolvere il problema, usare l'attributo **keymap** per mappare la keymap locale sul PC remoto.

Ad esempio, per impostare una mappatura della tastiera per il tedesco, utilizzare:

```
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
----------------------------------------------------------------------
```

Problemi noti relativi alle mappature della tastiera

- Cisco bug ID CSCth38454 - **Implementare la mappa chiave ungherese per il plug-in RDP.**
- ID bug Cisco CSCsu7600 - Le **chiavi della finestra del plug-in RDP WebVPN non sono corrette. Shift (tasto) .jar**.
- ID bug Cisco CSCtt04614 - **WebVPN - ES, segni diacritici della tastiera gestiti in modo non corretto dal plug-in RDP.**
- Cisco ID bug CSCtb07767 - **Plugin ASA - Configurazione dei parametri predefiniti**.

  Suggerimento: Per ovviare al problema, è inoltre possibile utilizzare uno Smart Tunnel dell'applicazione per **mstsc.exe.** Tale tunnel è configurato nella modalità di configurazione secondaria di WebVPN con il comando **smart-tunnel list RDP_List RDP mstsc.exe platform windows**.

Il plug-in Java RDP è in grado di supportare sessioni RDP a schermo intero?

Attualmente non è disponibile alcun supporto nativo per le sessioni RDP a schermo intero. La richiesta di miglioramento CSCto87451 è stata archiviata per implementare questa funzionalità. Se il parametro **geometry** (**geometry =1024x768**, ad esempio) è impostato sulla risoluzione del monitor utente, funziona in modalità a schermo intero. Poiché le dimensioni dello schermo variano, potrebbe essere necessario creare più collegamenti a segnalibri. Il client ActiveX supporta in modo nativo le sessioni RDP a schermo intero.

Il client Java è in grado di comunicare con l'uso di AES-256 per la crittografia?

Per consentire al client Java di negoziare correttamente il protocollo SSL, modificare l'ordine del set di cifrature SSL dell'ASA in modo che corrisponda a questo:

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

Il client Java potrebbe visualizzare questo errore se l'ordine del set di cifratura è diverso:

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

Risoluzione dei problemi RDP

Se si verificano altri problemi con il plug-in RDP, potrebbe essere utile raccogliere questi dati per risolvere i problemi relativi a RDP:

- L'output **show tech** dell'appliance ASA
- L'output **dettagliato del plug-in show import webvpn** dall'appliance ASA
- Il sistema operativo del computer dell'utente e le patch
- Sistema operativo del computer di destinazione e livello di patch
- Il client utilizzato (ActiveX o Java) e la versione Java JRE
- Determinare se l'ASA si trova in un cluster di bilanciamento del carico, basato su DNS o basato su ASA

Avvertenze note

Problemi relativi agli aggiornamenti per la protezione Microsoft

1. KB2695962 - Microsoft Security Advisory: Aggiornamento cumulativo per i kill bit ActiveX: 8 maggio 2012.
2. KB2675157 - MS12-023: Aggiornamento cumulativo della protezione per Internet Explorer: 10 aprile 2012.
3. cisco-sa-20120314-asaclient - Cisco ASA serie 5500 Adaptive Security Appliance VPN ActiveX senza client Controllo remoto Vulnerabilità dell'esecuzione del codice 14 marzo.

4. ID bug Cisco CSCtx68075 - Interruzione di ASA WebVPN con applicazione della patch di Windows KB2585542 (8.2.5.29 / 8.4.3.9).
5. KB2585542 - MS12-006: Descrizione dell'aggiornamento di protezione per WebIo, Winhttp e schannel in Windows: 10 gennaio 2012.

Client ActiveX

- **Sintomi:** Il client ActiveX non viene caricato dalle versioni 6-9 di IE dopo un aggiornamento al sistema operativo ASA versione 8.4.3.

  Fare riferimento all'ID bug Cisco CSCtx58556. La correzione è disponibile per le versioni 8.4.3.4 e successive.Soluzione temporanea: Imponi l'uso del client Java.

- **Sintomi:** Il caricamento del client ActiveX non riesce dopo il downgrade del sistema operativo ASA alla versione precedente alla 8.4.3. Questo problema interessa gli utenti che hanno usato il client ActiveX su un'appliance ASA con la correzione dell'ID bug Cisco CSCtx58556 e si connettono all'appliance ASA con una versione precedente alla 8.4.3. Questo problema è dovuto a un nuovo plug-in ActiveX RDP introdotto nell'appliance ASA versione 8.4.3, che non è compatibile con le versioni precedenti.

  Fare riferimento all'ID bug Cisco CSCtx57453.Rimuovere tutte le istanze del Registro di sistema di Windows relative a **b8e73359-3422-4384-8d27-4ea1b4c01232?** (vecchio CLSID ActiveX).

  Nota: È consigliabile eseguire un backup del Registro di sistema del computer prima di apportare modifiche.
- **Sintomi:** Le connessioni RDP ai dispositivi con NLA (Network Level Authentication) abilitato non riescono.

  Per ulteriori informazioni sul miglioramento che richiede l'integrazione di NLA nel plug-in ActiveX RDP, fare riferimento all'ID bug Cisco CSCtu63661.Anche se il client Microsoft ActiveX supporta NLA, l'uso di questa funzione nel plug-in ASA non è supportato.Soluzione. Configurare il plug-in RDP (**mstsc.exe**) in modo che disponga di un tunneling intelligente. Fare riferimento alla guida alla distribuzione della VPN SSL di Cisco ASA 5500, versione 8.x.

- **Sintomi:** Impossibile caricare ActiveX RDP. Verrà visualizzata una pagina vuota.

  Fare riferimento all'ID bug Cisco CSCsx49794.Questo si verifica quando la catena di certificati per il certificato SSL ASA è maggiore di quattro certificati (ad esempio, ROOT, SUBCA1, SUBCA2 e ASA CERT).Soluzione temporanea:

  Non installare la catena di certificati di grandi dimensioni sull'appliance ASA.Il plug-in Java RDP funziona correttamente, a differenza del plug-in ActiveX.Il protocollo RDP inoltre funziona correttamente quando si configura il file Windows **mstsc.exe** nativo con i tunnel intelligenti.

- **Sintomi:** Dopo aver utilizzato il client ActiveX RDP, l'utente fa clic sul pulsante **Logout** e riceve

un errore **HTTP 404 - Pagina non trovata**. Fare riferimento all'ID bug Cisco CSCtz3266. Il problema è stato risolto con il plug-in versione **rdp-plugin.120424.jar** o successive.

- **Sintomi:** In Internet Explorer sono aperte due schede, una per la sessione RDP e l'altra per una pagina Web vuota o di altro tipo. IE non funziona correttamente dopo la chiusura della scheda RDP.

  Fare riferimento all'ID bug Cisco CSCua69129.Soluzione temporanea: Utilizzare il plug-in Java RDP (Set **ForceJava=true**).

- **Sintomi:** Il plug-in ActiveX provoca un utilizzo elevato della CPU con IE. Fare riferimento all'ID bug Cisco CSCua16597.

- **Sintomi:** Dopo l'installazione dell'aggiornamento di Windows **KB2695962,** il plug-in ActiveX RDP non viene caricato. Quando viene aperta una nuova sessione RDP, il client ActiveX tenta di installare il server di inoltro della porta **VPN per SSL di Cisco** (ciò non accade sempre) e torna alla pagina del portale senza client senza connettersi al computer remoto. Ciò è dovuto alla vulnerabilità **CVE-2012-0358,** risolta sul lato client da Microsoft Security Advisory (2695962).

  Per ulteriori informazioni, fare riferimento al documento Cisco Security Advisory Cisco ASA serie 5500 Adaptive Security Appliance VPN ActiveX Control Remote Code Execution Vulnerability (Vulnerabilità dell'esecuzione del codice remoto per VPN senza client).Fare riferimento all'ID bug Cisco CSCtr00165.

Client Java

Nota: Cisco ridistribuisce i plug-in senza apportare modifiche. A causa della GNU General Public License, Cisco non modifica né estende l'applicazione plug-in. Il plug-in **JavaRDP appropriato** è un'applicazione open-source e qualsiasi problema relativo al software plug-in deve essere risolto dal proprietario del progetto.

- **Sintomi:** Le applicazioni a elaborazione intensiva vengono eseguite sul computer remoto quando vi si accede tramite il client Java RDP e si verifica un arresto anomalo dell'applet Java.

  Questo messaggio di errore potrebbe essere visualizzato: **FATAL net.propero.rdp - javax.net.ssl.SSLException: La connessione è stata chiusa: ....**Il comportamento viene attivato quando si passa rapidamente da un'applicazione ad uso intensivo di CPU all'altra.Questo problema è risolto nelle versioni plug-in rdp.2012.6.4.jar e successive. Soluzione temporanea:

  Connettersi utilizzando il client ActiveX.Non passare rapidamente da un'applicazione all'altra.

- **Sintomi:** Il client Java RDP genera questo messaggio di errore: **net.propero.rdp.Rdp - java.net.SocketException: Socket chiuso java.net.SocketException: Il socket viene chiuso** e quindi chiuso.

Il problema è causato da un gruppo del tunnel con un URL del gruppo configurato solo con il nome di dominio completo (ad esempio, http://www.example.com).Fare riferimento all'ID bug Cisco CSCuh72888.Soluzione temporanea:

Rimuovere la voce group-URL senza un "/" nel gruppo di tunnel.Utilizzare il client ActiveX.

- **Sintomi:** Java RDP Client non funziona quando è collegato a un computer Windows 8.

  Il client Java RDP non dispone attualmente del supporto per questa funzionalità.Fare riferimento all'ID bug Cisco CSCuc7990Soluzione temporanea:

  Utilizzare il client ActiveX RDP.Eseguire lo smart tunnel del client RDP nativo di Windows (**mstsc.exe**).

- **Sintomi:** Il client Java RDP non riesce con questo messaggio di errore: **EccezioneAssegnazioneAR: Trovata voce senza firma nella risorsa: https://10.105.130.91/+CSCO+3a75676763663A2F2F2E637968747661662E++/vnc/VncViewer.jar**.

  Questo problema è causato da un bug nel riscrittura Java di ASA webVPN.Fare riferimento all'ID bug Cisco CSCuj88114.Soluzione temporanea: Downgrade alla versione Java 7u40.