Notes relatives à la version 1.1.13 du micrologiciel pour Dispositifs de sécurité intégrés Cisco ISA500

Novembre 2012

Ces notes de version fournissent des informations importantes et décrivent des problèmes connus relatifs à la version du micrologiciel 1.1.13 .

IMPORTANT : comme pour toute version de micrologiciel, lisez attentivement ces notes de version avant de mettre à niveau le micrologiciel.

- Vous devez installer la version la plus récente du micrologiciel lors de la configuration d'un nouveau dispositif.
- Vous devez en outre mettre à niveau votre micrologiciel lorsqu'une nouvelle version de celui-ci est disponible.
- Il est recommandé de sauvegarder votre configuration avant de mettre à niveau le micrologiciel.

Table des matières

Ce document comprend les rubriques suivantes :

Remarques importantes

- L'utilitaire de configuration de la gamme ISA500 prend en charge les navigateurs Web suivants :
  - Microsoft Internet Explorer 8 et 9
  - Mozilla Firefox 3.6.x, 5 et 6
- Veuillez mettre à jour les signatures des fonctions Anti-virus et IPS si vous utilisez celles-ci. Pour plus d'informations, reportez-vous au guide *Cisco ISA500 Series Integrated Security Appliance Administration Guide* ou aux pages d'aide dans Security Services > Anti-Virus > General Settings and Security Services > Intrusion Prevention (IPS) > IPS Policy and Protocol Inspection.
- L'utilisation des versions suivantes du logiciel client Cisco AnyConnect Security Mobility est recommandée avec le modèle ISA500. Elles sont disponibles sur le CD contenant la documentation et le logiciel du produit Cisco ISA500.
  - anyconnect-EnableFIPS-win-3.0.2052.exe
  - anyconnect-linux-3.0.2052-EnableFIPS.tar.gz
  - anyconnect-linux-64-3.0.2052-EnableFIPS.tar.gz
  - anyconnect-macosx-i386-3.0.4235-EnableFIPS.tar.gz
  - anyconnect-macosx-i386-3.0.4235-k9.dmg
  - anyconnect-predeploy-linux-3.0.2052-k9.tar.gz
  - anyconnect-predeploy-linux-64-3.0.2052-k9.tar.gz
  - anyconnect-win-3.0.2052-pre-deploy-k9.iso
- Certains composants additionnels et modules d'extension Firefox sont incompatibles avec le micrologiciel. Si vous utilisez Firefox, Cisco recommande de désactiver les composants additionnels et modules d'extension suivants avant d'installer le micrologiciel :
  - Adblock Plus (composant additionnel)
  - bitcomentAgent (module d'extension)
  - WinZipBar (barre d'outils de navigateur)

Problèmes connus

Le tableau ci-après répertorie les problèmes connus de la version 1.1.13 . Comme pour toute mise à niveau, prenez-en connaissance avant de mettre à niveau votre micrologiciel.

Numéro de référence	Problème
CSCua43844	Le rapport d'utilisation (Usage Report) affiche parfois les adresses IP publiques au lieu des adresses IP privées sur le réseau local (LAN). Ce problème se produit généralement après un changement topologique, notamment pour les interfaces WAN.
CSCuc40174	L'interaction entre les protocoles STP (Spanning Tree Protocol) et CDP (Cisco Discovery Protocol) cause parfois une défaillance du trafic quand le protocole STP bloque un port du fait d'une boucle physique dans le réseau. **Solution de contournement :** supprimer la boucle physique ou désactiver le protocole STP, le protocole CDP ou les deux.
CSCuc47788	Le rapport d'utilisation de la bande passante par adresse IP (Bandwidth Usage Report by IP Address) affiche l'adresse IP publique du serveur au lieu de l'adresse IP du client SSLVPN.
CSCuc89697	Les téléphones mobiles utilisant AnyConnect Mobile Client se déconnectent parfois.
CSCud06033	Quand la priorité VRRP est modifiée, la mise à jour n'est pas envoyée au PC. Par exemple, après l'ajustement de la priorité pour qu'un routeur serve de sauvegarde, les deux routeurs agissent parfois comme routeurs principaux. **Solution de contournement :** désactiver le protocole STP.

Numéro de référence	Problème
CSCud10160	Les processus UPNP peuvent provoquer l'exécution du processeur à 100 %. **Solution de contournement :** ouvrir la page Device Management > Discovery Protocols > UPnP, désactiver UPnP, puis le réactiver.
CSCub91801	Avec les versions AnyConnect 3.1.00496 ou supérieures, la connexion VPN SSL s'interrompt parfois durant la renégociation MTU. **Solution de contournement :** attribuer la valeur par défaut 1 500 à la taille MTU sur le PC.

Informations connexes

Assistance	
Communauté d'assistance Cisco Small Business	www.cisco.com/go/smallbizsupport
Assistance et ressources CiscoSmallBusiness	www.cisco.com/go/smallbizhelp
Coordonnées de l'assistance téléphonique	www.cisco.com/go/sbsc
Téléchargement de micrologiciels CiscoSmallBusiness	www.cisco.com/go/isa500software
Requêtes Open Source Cisco Small Business	www.cisco.com/go/smallbiz_opensource_request
Documentation	
Documentation sur les produits	www.cisco.com/go/isa500resources

CiscoSmallBusiness	
Site Cisco Partner Central pour les petites entreprises (connexion partenaire requise)	www.cisco.com/web/partners/sell/smb
Accueil Cisco Small Business	www.cisco.com/smb

78-21121-01