

# Release Notes for SRP520 Series Services Ready Platforms Software Version 1.01.26

These Release Notes describe the open and resolved issues with the SRP520 Series Services Ready Platforms (SRP521W, SRP526W, SRP527W) software version 1.01.26, and includes the changes since version 1.01.24.

This document includes the following topics:

- **New Features**
- **Limitations and Restrictions**
- **Open Issues**
- **Resolved Issues**
- **Related Information**

## New Features

The following new features were introduced since software version 1.01.24:

- Support for Cisco VPN Server for use with the Cisco VPN Client v5.0 or later.
- Added 1/32 to VPI/VCI auto-detect list. The entire list now includes: 1/32, 0/38, 0/35, 8/35, 0/43, 0/51, 0/59, 8/43, 8/51, and 8/59.
- Added support for the following USB modems:
  - Huawei E173, E352, E372 (HSPA)
  - Pantech UML290 (CDMA Rev.A/LTE)
  - Sierra Wireless AC320U (HSPA+/LTE)
  - ZTE K3805-Z, K4505-Z, MF112, MF636DB (HSPA)
  - ZTE AC2726, AC2736 (CDMA EVDO Rev. A)

For a complete list of supported modems, see the Mobile Broadband USB Modem Compatibility Matrix (SRP520 Models) located under Technical References at: [www.cisco.com/go/srp500resources](http://www.cisco.com/go/srp500resources).

## Limitations and Restrictions

These are the limitations and restrictions for the SRP520 Services Ready Platforms. These are known limitations that may not be fixed or may not have a workaround.

- The FXS interface is unable to send packets directly to a LAN side IP phone, resulting in 1-way audio from the IP phone to the FXS interface.

The workaround is to enable SIP ALG on the SRP. On the LAN side IP phone, set **<NAT Mapping Enable> = no** on its Ext tab. (CSCti44955)

- Silent audio on a call placed between the ATA's FXS1 and FXS2 interfaces. This problem occurs when the ATA is added to the SRP's LAN site, and SIP ALG is enabled on the SRP.

The workaround is to disable SIP ALG and use a port forwarding rule for the ATA's NAT traversal instead. (CSCti50573)

- Call placed between an ATA phone (configured with remote ringback) and the SRP results in 1-way audio. This problem occurs when SIP ALG is enabled on the SRP, and no port forwarding rules are configured.

The workaround is to disable SIP ALG and use a port forwarding rule for NAT traversal instead. (CSCtl55029)

- SIP attack causes latency and bad voice quality.

The workaround is to restrict Source IP from the *Voice > Line 1-2 > SIP Setting* page. Select **yes** for Restrict Source IP. (CSCto75874)

## Open Issues

The following table lists the open issues in software version 1.01.26:

Ref Number	Description
CSCtj37034	<p>After changing the remote IP address for the IPSec policy from the <i>VPN &gt; IPSec Policy</i> page, the SRP is unable to reconnect to the VPN tunnel.</p> <p><b>Workaround</b> Disable and then re-enable the VPN tunnel.</p>
CSCtl21714	<p>FXO not working properly when the WAN (Internet) is disconnected.</p> <p><b>Workaround</b> None.</p>
CSCtn91639	<p>FXS1 port can relay to the FXO port during a power outage and establish a PSTN call, but call is dropped when re-registering to the proxy.</p> <p><b>Workaround</b> None.</p>
CSCto05295	<p>When the SRP dials *99+ (callee ID) and places a modem call, it advertises all supported codecs (g711u, g729, g711a, and g726-32).</p> <p><b>Workaround</b> None.</p>

## Release Notes

---

Ref Number	Description
CSCtq53805	SRP fails to transfer a file though a modem call connection. This occurs because the transfer connection exceeds the error limits or connection timeout. <b>Workaround</b> None.
CSCty04890	FTP session drops when the DHCP lease is renewed. <b>Workaround</b> Reinstate the FTP session.
CSCtx90063	LAN side host obtains TFTP server address through DHCP option 66, even though the WAN server does not provide it. <b>Workaround</b> None.

## Resolved Issues

The following issues were resolved since software version 1.01.24:

Ref Number	Description
CSCtk56567	Destination_Mode tag under DMZ appears twice in the XML configuration.
CSCtq33773	FXS1 port can relay to the FXO port during a power outage and establish a PSTN call, but call is dropped when power is restored.
CSCtq95702	WPS settings are not applied after configuring an SSID with WPS from the <i>Interface setup &gt; Wi-Fi Settings &gt; Basic Wireless Settings</i> page.
CSCtr41192	Illegal IP address message occurs when the VPN Server DHCP IP Pool address is set to 15.15.15.0.
CSCts34329	When PPTP starts the connection, the SRP uses the hardcoded hostname instead of the hostname assigned manually through the Configuration Utility.
CSCts28580	The SRP's EoA interface stops forwarding traffic after 5-6 days.

Ref Number	Description
CSCts65054	New VLAN unable to access the Internet through a 3G connection.
CSCtt05930	Daylight savings rule is incorrect for New Zealand.
CSCtt46871 CSCtw55495 CSCtw56009	<p>Cisco SRP520 Series Services Ready Platforms contain the following three vulnerabilities:</p> <ul style="list-style-type: none"> <li>▪ Web Interface Command Injection Vulnerability.</li> <li>▪ Unauthenticated Configuration Upload Vulnerability.</li> <li>▪ Directory Traversal Vulnerability.</li> </ul> <p>These vulnerabilities can be exploited using sessions to the Services Ready Platform Configuration Utility web interface. These vulnerabilities could be exploited from the local LAN side of the SRP device by default configuration and the WAN side of the SRP device if remote management is enabled. Remote management is disabled by default.</p> <p>Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.</p> <p>This advisory is available at the following link:  <a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120223-srp500">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120223-srp500</a> </p>
CSCtx25863	The default setting for WPS is disabled, but shows as enabled on the <i>Interface Setup &gt; Wi-Fi Settings &gt; Basic Wireless Settings</i> page.
CSCtx54914	SNMP does not report the system uptime correctly.
CSCtx84926	Device reboot warning message does not appear after configuring a static DNS address.
CSCtx90075	SRP cannot obtain an IP address in PPPoE mode after importing an XML file.
CSCtt42339	Cannot create IPSec policy due to IKE index error.

## Related Information

Support	
Cisco Small Business Support Community	<a href="http://www.cisco.com/go/smallbizsupport">www.cisco.com/go/smallbizsupport</a>
Online Technical Support and Documentation (Login Required)	<a href="http://www.cisco.com/support">www.cisco.com/support</a>
Cisco Small Business Support and Resources	<a href="http://www.cisco.com/go/smallbizhelp">www.cisco.com/go/smallbizhelp</a>
Phone Support Contacts	<a href="http://www.cisco.com/go/sbsc">www.cisco.com/go/sbsc</a>
Software	
Software Downloads (Login Required)	<a href="http://www.cisco.com/go/srp500">www.cisco.com/go/srp500</a> Click the Download Software link.
Open Source Documentation	<a href="http://www.cisco.com/en/US/products/ps10500/prod_release_notes_list.html">www.cisco.com/en/US/products/ps10500/prod_release_notes_list.html</a>
Product Documentation	
Cisco Services Ready Platform 500 Series for Small Business	<a href="http://www.cisco.com/go/srp500resources">www.cisco.com/go/srp500resources</a>
Regulatory Compliance and Safety Information	<a href="http://www.cisco.com/en/US/products/ps10500/prod_installation_guides_list.html">www.cisco.com/en/US/products/ps10500/prod_installation_guides_list.html</a>
Cisco Small Business	
Cisco Partner Central for Small Business (Partner Login Required)	<a href="http://www.cisco.com/web/partners/sell/smb">www.cisco.com/web/partners/sell/smb</a>
Cisco Small Business Home	<a href="http://www.cisco.com/smb">www.cisco.com/smb</a>
Marketplace	<a href="http://www.cisco.com/go/marketplace">www.cisco.com/go/marketplace</a>

Cisco, Cisco Systems, the Cisco logo, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

© 2012 Cisco Systems, Inc. All rights reserved.

78-20719-01