Product Correction Notice (PCN)

Issue Date:	**February 22, 2008**
Archive Date:	**Not Applicable**
Supplement 2 Date:	**August 15, 2008**
PCN Number:	**1625P**

SECTION 1 - CUSTOMER NOTICE

This PCN addresses issues with the following products and systems:

Avaya S8xx0 Servers running Communication Manager 3.x (fix only available on Communication Manager 3.1.4 and later), 4.x and 5.x releases.

Does this PCN apply to me?

This Correction Notice applies **only to customers that are currently running Communication Manager 3.x (R013x.00.0.340.3 and later), 4.x (R014x.00.0.730.5 through R014x.00.1.731.2) or 5.0 (R015x.00.0.825.4) software loads**. Customers with Communication Manager 3.x release versions prior to 3.1.4 who are looking to resolve issues addressed by this PCN must upgrade to Communication Manager 3.1.4 load R013x.01.4.642.1 (per PCN 1523B) before installing the 3.1.4 security patch or upgrade to a release later than Communication Manager 3.1.4.

This PCN introduces security service pack #1 for Communication Manager 4.x/5.x. It also introduces a patch for Communication Manager 3.1.4 on Avaya S8xx0 Servers.

The security service pack, PLAT-rhel4-1000.tar.gz, applies concurrently with any other Communication Manager patches or service packs to S8xx0 series Servers running either Communication Manager 4.x (R014x.00.0.730.5 through R014x.00.1.731.2) or 5.0 (R015x.00.0.825.4). The security service pack is only applicable to Communication Manager servers with release versions 4.x/5.0.

The Communication Manager 3.1.4 patch (01.4.642.1-15179.tar.gz) containing the same security fix that is included in security service pack PLAT-rhel4-1000 is a special Communication Manager 3.1.4 load 642.1 patch that may be applied concurrently with any other patches or service packs.

What you should do when you receive this PCN:

If you are currently running a Communication Manager 3.x release prior to Communication Manager 3.1.4, you should upgrade to Communication Manager 3.1.4 per PCN 1523B and install the specified Communication Manager 3.1.4 security patch on all applicable Servers. If you are running a release later than Communication Manager 3.1.4, you do not need to install the specified security patch. If you are running Communication Manager 4.0/4.0.1/5.0, you should install the specified security service pack on all applicable Servers. If you are running a Communication Manager 4.x release later than 4.0.1 (R014x.00.1.731.2) or a Communication Manager 5.x release later than 5.0 (R015x.00.0.825.4), you do not need to install the specified security service pack.

Description of PCN:	This notice specifies Communication Manager 3.1.4 patch 01.4.642.1-15179 and Communication Manager 4.x/5.0 security service pack PLAT-rhel4-1000 Software Update Procedures. The security patch or security service pack should be installed on all applicable S8xx0 Servers running the applicable release of Communication Manager 3.1.4/4.x/5.0.
What is the nature of the PCN?	Communication Manager 3.1.4 software security patch and 4.x/5.0 software security service pack number 1 for Avaya S8xx0 Servers.
This PCN addresses and resolves the following issues:	Avaya's monitoring of the Red Hat Linux security advisory alert system has uncovered a number of Medium Risk security vulnerabilities that affect Communication Manager. Avaya Security Advisories created to detail these vulnerabilities may be found at http://support.avaya.com/security. The Avaya Security Advisories created to address security issues covered by this PCN include ASA-2007-488, ASA-2007-493 and ASA-2007-505.
Level of Risk/Severity Class 1=High Class 2=Medium Class 3=Low	Class 3
Is it required that this PCN be applied to my system?	This PCN is required for S8xx0 series Servers running Communication Manager 3.x (R013x.00.0.340.3 and later), 4.x (R014x.00.0.730.5 through R014x.00.1.731.2) or 5.0 (R015x.00.0.825.4) software loads. Systems running Communication Manager 3.x releases prior to 3.1.4 must first upgrade to Communication Manager 3.1.4 per PCN 1523B. Systems running a release later than Communication Manager 3.1.4 for 3.x, 4.0.1 for 4.x or 5.0 for 5.x do not need to install the specified security patch or service pack.
The risk if this PCN is not installed:	The Avaya Security Advisories addressed by this PCN outline the potential risk if the latest security fixes are not applied to a system.
Is this PCN for US customers, non-US customers, or both?	This applies to both US and non-US customers.
Does applying this PCN disrupt my service?	Please refer to PCN 1523B for any service disrupting notes when upgrading to Communication Manager 3.1.4 if an upgrade is required. Installation of the Communication Manager 3.1.4 security patch or Communication Manager 4.x/5.0 security service pack is not service disrupting.
Installation of this PCN is required by:	Customer or Avaya Authorized Service Provider. Both the security patch and security service pack are customer installable and remotely installable.

Release notes and workarounds are located:

Avaya Security Advisories created to detail the vulnerabilities addressed in this PCN may be found at http://support.avaya.com/security. This PCN covers the following Avaya Security Advisories: ASA-2007-488, ASA-2007-493 and ASA-2007-505.

The security service pack itself contains references to specific Avaya Security Advisories it addresses. This information may be obtained on a Communication Manager 4.x/5.0 system by executing the command "update_info PLAT-rhel4-1000" from the bash shell after the security service pack has been unpacked.

How to determine if your product is affected:

All S8xx0 series Servers running Communication Manager 3.x (fix only available on Communication Manager 3.1.4), 4.0, 4.0.1 and 5.0 software are affected. Servers running a release later than Communication Manager 3.1.4, 4.0.1 or 5.0 are not affected and therefore do not require the specified security patch or security service pack.

To determine the release of Communication Manager software that is being run on a server you can execute the *swversion* command from the bash shell or execute a *list configuration software-versions* command from the SAT.

Required materials (If PCN can be customer installed):

This PCN is being issued as a customer installable PCN. Either Communication Manager security patch 01.4.642.1-15179.tar.gz or security service pack PLAT-rhel4-1000.tar.gz is required. To obtain the security patch or security service pack, refer to the **Provisioning Instructions** section of this PCN.

If unfamiliar with installing Communication Manager patches or security service packs, the installation instructions are required. To obtain the installation instructions please refer to the **Finding the installation instructions** section of this PCN.

Provisioning instructions (If PCN can be customer installed):

The security patch for Communication Manager 3.1.4 (01.4.642.1-15179.tar.gz) and security service pack PLAT-rhel4-1000.tar.gz can be obtained by performing the following steps from a browser:

1. Go to http://support.avaya.com and click **Downloads**
2. Click on **Latest TN Circuit Pack, Media Server, and Media Gateway Firmware and Software Updates**
3. Click on GA load **730.5/731.2/825.4** for the **Communication Manager 4.0/4.0.1/5.0** release or GA load **642.1** for the **Communication Manager 3.1.4** release in the Release row of the **Security Update table for Media Servers running Communication Manager.**
4. Click on the file name link (**PLAT-rhel4-1000.tar.gz**) below **Latest Avaya Communication Manager 4.0/4.0.1/5.0 Security Service Pack** to access the security service pack download. To access the **Communication Manager 3.1.4** security patch click on the link **01.4.642.1-15179.tar.gz**.

The MD5 sum for the **Communication Manager 3.1.4** security patch is:
c2d5baa8ccebb5ba4cd462245fce91ff

The MD5 sum for the **Communication Manager 4.x/5.0** security service pack is:

21bd99895e653e58b103f998eab798ef

Finding the installation instructions (If PCN can be customer installed):

This PCN is being issued as a customer installable PCN. The security patch, service pack and security service pack installation instructions can be obtained by performing the following steps from a browser:

1. Go to http://support.avaya.com and click **FIND DOCUMENTATION and TECHNICAL INFORMATION by PRODUCT NAME**
2. Click on the **S8xx0 Server** of interest
3. Click on **Installation, Migrations, Upgrades and Configurations**
4. Click on **Upgrading, Migrating and Converting Media Servers and Gateways** to open up document
5. Search for **Installing security and Communication Manager service pack updates** for detailed instructions on how to install the security service pack or patch on the Server.

SECTION 1A – PATCH INFORMATION

Note: Customers are required to backup their systems before applying the Patch.

How to verify the installation of the patch has been successful:

To verify the security patch or security service pack is successfully installed perform the following steps from a web browser:

1. Access the Server web pages by entering the Server name or IP address in the browser Address box.
2. Login to the web pages.
3. Click on **Launch Maintenance Web Interface**.
4. Click on **Software Version** under the **Server** heading.
5. For Communication Manager 3.1.4, verify under "UPDATES:" that the patch containing the security fix shows "activated".
6. For Communication Manager 4.x/5.0, verify under "UPDATES:" that the security service pack "PLAT-rhel4-1000" shows "activated".

Alternatively, run the following bash command on the Media Server:

```
> update_show
```

This should show the status of the security patch (Update ID) or security service pack (Platform/Security ID) "PLAT-rhel4-1000" as "activated".

What you should do if the patch installation fails?

Escalate to Avaya GSD General Business Service Desk (800-242-2121).

How to remove the patch if malfunction of your system occurs:

For Communication Manager 3.1.4, run the following bash command on the Server:

```
> update_deactivate 01.4.642.1-15179
```

For Communication Manager 4.x/5.0, run the following bash command on the Server:

```
> update_deactivate PLAT-rhel4-1000
```

After the command has completed run the following bash command on the Media Server:

```
> update_show
```

This should show the status of the security patch (Update ID) or security service pack (Platform/Security ID) "PLAT-rhel4-1000" as "deactivated".

NOTE: Deactivating the security patch or security service pack alone may not restore the system to its previous state. If activation or deactivation of a security patch or security service pack fails, please contact the Avaya GSD General Business Service Desk to ensure that the packages installed on the system have been correctly restored.

SECTION 1B – SECURITY INFORMATION

Are there any security risks involved?

Avaya’s monitoring of the Red Hat Linux security advisory alert system has uncovered a number of Medium Risk security vulnerabilities that affect Communication Manager. Avaya Security Advisories created to detail these vulnerabilities may be found at http://support.avaya.com/security. The Avaya Security Advisories created to address security issues covered by this PCN include ASA-2007-488, ASA-2007-493 and ASA-2007-505.

Avaya Security Vulnerability Classification:

Under Avaya's Security Vulnerability Classification policy, the issues addressed by this PCN are rated at a Medium risk.

Mitigation:

Taking advantage of known vulnerabilities in Communication Manager requires access to Avaya maintenance web pages or a system shell prompt, both of which are restricted to active user accounts only. Avaya recommends that account access be restricted to only those who require usage of the system.

Material Coverage Entitlements:

There is no charge for the material in this PCN. The Communication Manager 3.1.4 security patch and Communication Manager 4.x/5.0 security service pack are available on support.avaya.com.

Avaya Customer Service Coverage Entitlements:

Avaya is issuing this PCN as remotely installable by the customer. If the customer requests Avaya to install this PCN, it is considered a billable event as outlined in Section 4 (*Software Updates and Product Correction Notices*) of the Avaya Service Agreement Supplement (Full Maintenance Coverage) unless the customer has purchased an Avaya Services enhanced offer such as the Avaya Services Product Correction Support offer.

Additionally, Avaya on-site support is not included. If on-site support is requested, Avaya will bill the customer current Per Incident charges unless the customer has purchased an Avaya Services enhanced offer such as the Avaya Services Product Correction Support offer.

Customers under the following Avaya coverage: -Warranty -Full Coverage Service Contract* -On-site Hardware Maintenance Contract*	
Remote Installation	Current Per Incident Rates Apply
On-site Technician Labor	Current Per Incident Rates Apply

* Service contracts that include both labor and parts support – 24x7, 8x5.

Customers under the following Avaya coverage: -Software Support -Software Support Plus Upgrades -Remote Only -Parts Plus Remote -Remote Hardware Support -Remote Hardware Support w/ Advance Parts Replacement	
Remote Installation	Current Per Incident Rates Apply
On-site Technician Labor	Current Per Incident Rates Apply

Per Incident Customer **(No Avaya Warranty or Avaya Service Contract)**	
Remote Installation	Current Per Incident Rates Apply
On-site Technician Labor	Current Per Incident Rates Apply

Avaya Product Correction Notice Support Offer
The Avaya Product Correction Support Offer provides out-of-hours support for remote and on-site technician installable PCNs, and Avaya installation for all Avaya issued PCNs that are classified as "Customer-Installable". Refer to the PCN Offer or contact your Avaya Account Representative for complete details.

Avaya Authorized BusinessPartner Service Coverage Entitlements:

Authorized BusinessPartner
Avaya authorized BusinessPartners are responsible for the implementation of this PCN on behalf of their customers. Any support or work performed by Avaya may result in Per Incident charges.

Avaya Contact List:

Avaya Contact	Telephone Number
GSD General Business Service Desk	800 – 242 - 2121
Canada Customer Care Center	800 – 387 - 4268
Remote Service Center – Hungary	361 - 345 - 4334
Caribbean and Latin America	786 – 331 - 0860
EMEA Services - Post Sales Technical Support	31-70-414-8720
Asia/Pacific Regional Support Center	+800-2-28292-78 / +65 6872 5141 and +008006501243 (India)