Product Correction Notice (PCN)

Issue Date: February 29, 2008
Archive Date: Not Applicable
PCN Number: 1626P

SECTION 1 - CUSTOMER NOTICE

This PCN addresses issues with the following products and systems:

Avaya SIP Enablement Services 4.0 deployed on S8500 series servers and Avaya SIP Enablement Services 5.0 deployed on S8500 or S8300C servers.

Does this PCN apply to me?

This Correction Notice applies only to customers that are currently running SIP Enablement Services 4.0 and/or 5.0 software loads.

SIP Enablement Services 4.0 Service Pack 2a (04.0.033.6-SP2a.tar.gz) applies to customers running SIP Enablement Services 4.0 on the S8500 series servers. Customers running versions prior to SIP Enablement Services 4.0 must first upgrade to release 4.0 before applying this Service Pack.

SIP Enablement Services 5.0 Security Service Pack 1 (PLAT-rhel4-1000.tar.gz) applies to customers running SIP Enablement Services 5.0 on the S8500 series or S8300C servers and can be applied concurrently with any other release 5.0 Service Packs.

What you should do when you receive this PCN:

If you are currently running a SIP Enablement Services release prior to 4.0, you should upgrade to SIP Enablement Services software release 4.0 and then install Service Pack 2a (04.0.033.6-SP2a.tar.gz).

SIP Enablement Services 4.0 Service Pack 2a should be installed on all servers running SIP Enablement Services 4.0.

SIP Enablement Services 5.0 Security Service Pack 1 should be installed on all S8500 series servers and S8300C servers running SIP Enablement Services 5.0.

Description of PCN:

This notice specifies SIP Enablement Services 4.0 Service Pack 2a (04.0.033.6-SP2a.tar.gz) and SIP Enablement Services 5.0 Security Service Pack 1 (PLAT-rhel4-1000.tar.gz) Software Update Procedures.

These service packs should be installed on all servers running the applicable release of SIP Enablement Services.

What is the nature of the PCN?

SIP Enablement Services 4.0 Service Pack 2a and SIP Enablement Services 5.0 Security Service Pack 1.

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 SIP Enablement Services. 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 SIP Enablement Services 4.0 deployed on Avaya S8500 series servers and for SIP Enablement Services 5.0 deployed on S8500 series or S8300C servers. Customers running earlier release of SIP Enablement Services must minimally upgrade to release 4.0 before installing the appropriate 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?	Installation of the service pack or security service pack themselves is not service disrupting.
Installation of this PCN is required by:	Customer or Avaya Authorized Service Provider. SIP Enablement Services 4.0 Service Pack 2a and SIP Enablement Services 5.0 Security Service Pack 1 are both 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 SIP Enablement Services 5.0 system by executing the command "update_info PLAT-rhel4-1000" from the bash shell after the security service pack has been unpacked. Release notes are available for SIP Enablement Services 4.0 Service Pack 2a at http://support.avaya.com/japple/css/japple?PAGE=ProductIndex link to SIP Enablement Services Release 4.0.

How to determine if your product is affected:

All SIP Enablement Services 4.0 and 5.0 servers are affected.

To determine the release of SIP Enablement Services software that is being run on a server you can execute the *swversion* command from the bash shell or display via the Maintenance Web Page by clicking on the Software Version link.

Required materials (If PCN can be customer installed):

This PCN is being issued as a customer installable PCN.

SIP Enablement Services 4.0 Service Pack 2a (04.0.033.6-SP2a.tar.gz) is required for customers running SIP Enablement Services 4.0.

SIP Enablement Services 5.0 Security Service Pack 1 (PLAT-rhel4-1000.tar.gz) is required for customers running SIP Enablement Services 5.0.

To obtain the service pack or security service pack, refer to the **Provisioning Instructions** section of this PCN.

If unfamiliar with installing SIP Enablement Services service packs 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):

SIP Enablement Services 4.0 Service Pack 2a (04.0.033.6-SP2a.tar.gz) and SIP Enablement Services 5.0 Security Service Pack 1 (PLAT-rhel4-1000.tar.gz) can be obtained by performing the following steps from a web browser:

1. Go to http://support.avaya.com and click **Downloads**
2. Click on **SIP Enablement Services**
3. Click on **Select a Release from the drop down menu.**
4. Click on **Latest Avaya SIP Enablement Server 5.0 Security Service Pack** to access the security service pack download for SIP Enablement Services 5.0 or on **Avaya SIP Enablement Services Release 4.0 Service Pack 2a** for SIP Enablement Services 4.0

The MD5 sum for the SIP Enablement Services 5.0 Security Service Pack 1 is:

21bd99895e653e58b103f998eab798ef

The MD5 sum for the SIP Enablement Services 4.0 Service Pack 2a is:

0f1c5d40f4f694508ed20a5d4bfba039

Installation instructions:

3 Steps are required to install a service pack on SIP Enablement Services. The service pack must be

- copied to the Avaya S8xx0 Servers running SIP Enablement Services,
- unpacked on the Avaya S8xx0 Servers running SIP Enablement Services
- activated on the Avaya S8xx0 Servers running SIP Enablement Services

These steps can be executed via the SIP Enablement Services maintenance web pages or via the command line interface.

To apply via the SIP Enablement Services maintenance web pages, launch the maintenance web server interface then:

Click download files:

- provide the location of the updated file on the local PC or the web URL
- click download

Click manage updates:

- select the desired update and choose unpack
- select the desired update and choose activate

To use the command line interface:

- Use secure ftp to copy the update into /var/home/ftp/pub on the SIP Enablement Services server
- Use ssh to login to the SIP Enablement Services Server
- Execute update_unpack and select the desired update from the displayed list
- Execute update_activate “update-name”, substituting “update-name” with the name of the update

SECTION 1A – SERVICE PACK INFORMATION

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

How to verify the installation of the service pack has been successful:

To verify the service pack 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 SIP Enablement Services 4.0, verify under "UPDATES:" that the service pack containing the security fix shows "activated".
6. For SIP Enablement Services 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 service pack (Update ID) or security service pack (Platform/Security ID) "PLAT-rhel4-1000" as "activated".

What you should do if the service pack installation fails?

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

How to remove the service pack if malfunction of your system occurs:

For SIP Enablement Services 4.0, run the following bash command on the Server:

> update_deactivate 04.0.033.6-SP2a

For SIP Enablement Services 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 service pack (Update ID) or security service pack (Platform/Security ID) "PLAT-rhel4-1000" as "deactivated".

NOTE: Deactivating the service pack or security service pack alone may not restore the system to its previous state. If activation or deactivation of a service pack 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 SIP Enablement Services 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 SIP Enablement Services 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. SIP Enablement Services 4.0 Service Pack 2a and SIP Enablement Services 5.0 Security Service Pack 1 are both 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
Remote Service Center – Hungary	361 - 345 - 4334
Caribbean and Latin America	786 – 331 - 0860
EMEA Services	31-70-414-8720
Asia / Pacific Regional Support Center	+800-2-28292-78 / +65 6872 5141 and +008006501243 (India)