Product Support Notice

PSN #	PSN004105u

Original publication date: 11-Dec-13; This is Issue #02, published date: 16-Dec-13.	Severity/risk level	High	Urgency	Immediately

Name of problem	IP Office Unified Communications Module (UCM) goes into ‘write protect’ mode and Preferred Voice mail shuts down

Products affected

Unified Communications Module (700501442) with serial numbers from 13WZ31xxxxxx and 13WZ43xxxxxx
IP Office Release 8.1 and IP Office Release 9.0 are supported releases for this patch

Problem description

In certain scenarios, the Solid State Drive (SSD) on the UCM goes into ‘write protect’ mode as early as a few weeks of use. Impacted UCMs can shut down the Preferred Edition Voicemail operation. The units exhibiting this issue would have a PCS level 9 for the UCM unit and PCS level 04 for the on-board SSD drive. The PCS level for the UCM unit can be located on either the UCM shipping box (see figure 1 below) or on the UCM module itself (see figure 2). The PCS for the on-board SSD drive is located on the top right of the blue sticker that is attached to the drive (see figure 3).

Figure 1.

Figure 2

Figure 3

Resolution

A PSN is being issued to address the fault that causes the SSD to revert to 'write protect' (WP) mode due to a microcontroller firmware deficiency. Other components and performance of the IP Office control unit are not impacted.

The corrective action is to install a Critical Patch (CP) on the UCM through the UCM WebControl Application. The Critical Patch can be found at http://support.avaya.com. Tech Tip #258 is also available

This corrective action should be performed on all Unified Communications Modules that meet the serial number and PCS level prerequisites. Repair/maintenance units supplied through the RMA process will also need to apply the patch. Repair/maintenance units will not follow the serial numbers for the UCM as indicated above; the SSDs have been replaced during repair with SSD PCS 04 versions and need to follow the corrective action. Failure to perform this corrective action will leave the UCM vulnerable to incorrectly lock into a 'write protect' (WP) mode and cause the Preferred Edition Voicemail to shut down. There is a possible risk of data loss if the unit goes into WP mode and this procedure is not performed.

Determining if the Critical Patch should be deployed

There are three situations that require that the Critical Patch (CP) be installed on the UCM.

1. UCM installed (no issue): If the serial number of the installed UCM falls within the range of potentially-affected units, we recommend that the software fix is downloaded and installed on the UCM per the provided instructions.
2. UCM purchased but not yet implemented: Avaya recommends that the software fix be downloaded and installed on any existing current non-implemented UCM stock in your inventory.
3. UCM units that are received coming from Repair/Distribution due to a RMA/DOA replacement: Avaya recommends that software fix be downloaded and installed on all UCM's that are received from Repair/RMA/DOA replacement. This includes PCN1920h replacements with SSD PCS 04.

If your UCM is installed and is currently experiencing this issue the UCM must be replaced. Avaya recommends that our channel partners file an escalation ticket. Partners may elect to follow the RMA/DOA process, if necessary. Additionally, if the customer account has an IP Office Support Services (IPOSS) with Advanced Parts Replacement (APR) contract they can follow the documented IPOSS process.

Workaround or alternative remediation

n/a

Remarks

n/a

Patch Notes

The information in this section concerns the patch, if any, recommended in the Resolution above.

Backup before applying the patch

The SSD Firmware Update Critical Patch in itself does not destroy current data that may be stored on the SSD drive. However, it is

Avaya's recommendation that if there is customer Voicemail or one-X Portal data residing on a Unified Communications Module (UCM) it should be backed up onto a remote server or drive following the standard backup procedures outlined in the Administering Voicemail Pro Guide and one-X Portal for IP Office Guide before proceeding with the installation of the SSD Firmware Update Critical Patch.

Download

Required Software:

1. SSDFWUpgrade-1.0.0.-7.zip patch located on http://support.avaya.com
2. Access to the UCM WebControl Application

Patch install instructions — Service-interrupting?

Yes

Critical Patch Installation Instructions for Release 8.1 UCM's

1. Launch the WebControl Application and login as Administrator.
2. In the 'Settings' tab, load the zip file in the Applications Software Repositories by browsing to the zip file and then press the 'Add' button.
3. In the 'Updates' tab under the 'Services' window install the new .rpms in the following order:
   a. mailx
   b. smartmontools
   c. SSDFWUpgrade

   Note: the SSD Firmware Upgrade package will NOT install properly if mailx and smartmontools are not installed first!
4. Upon successful completion of the SSD Firmware Upgrade package the UCM will automatically power down. For cases where the SSD Firmware Upgrade is not required the installation of the .rpm files will not effect the system.
5. The UCM can be restarted via the System Status Application (SSA) (see figure 5) or by pressing the top button on the UCM module.

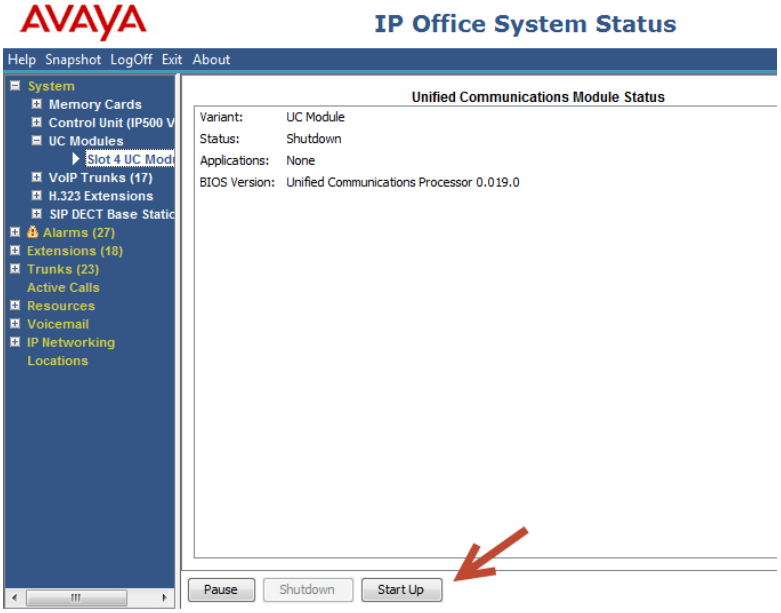

Figure 5

Once the UCM has completed the start-up process the diagnostic information will be displayed in the System Status Application (SSA) (see figure 6).

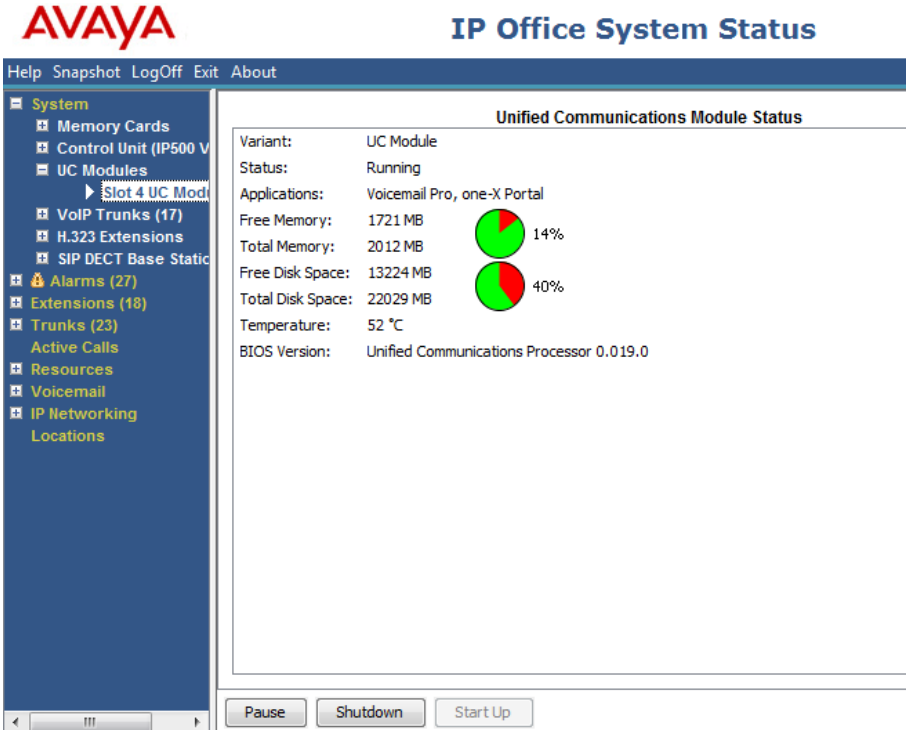

Figure 6

6. The success of the SSD Firmware package can be confirmed by viewing the 'Notifications' window on the WebControl Applications 'Home' tab. This will show three possible messages depending on the SSD version that is installed in the UCM.
    a. 'SSD Firmware not needed. SSD version is Ver703.o'.
    b. 'SSD Firmware not needed. SSD version is S5FAR031'.
    c. 'SSD Firmware upgrade successful. Power cycle was completed to finalize the changes'.
    d. 'SSD Firmware upgrade failed'. **In this case, the UCM should be replaced.**

    All of these messges are acceptable.
7. At this point the Unified Communications Module (UCM) SSD Firmware Upgrade has been completed successfully. You may now put the UCM into service.

Critical Patch Installation Instructions for Release 9.0 UCM's

1. Launch the WebControl Application and login as Administrator.
2. In the 'Settings' tab, load the zip file in the Applications Software Repositories by browing to the zip file and then press the 'Add' button.
3. Browse to the 'Updates' tab and wait for all of the Services to load. **There are two possible scenerios for installing the SSDFWUpgrade Critical Patch. This will depend on the method that was used to upgrade the UCM to 9.0 when it was originally installed. If the mailx.rpm and the smartmontools.rpm show that they are 'Up to Date' then you may proceed with the installation of the SSDFWUpgrade by pressing the Install radio button. (see Figure 7)**

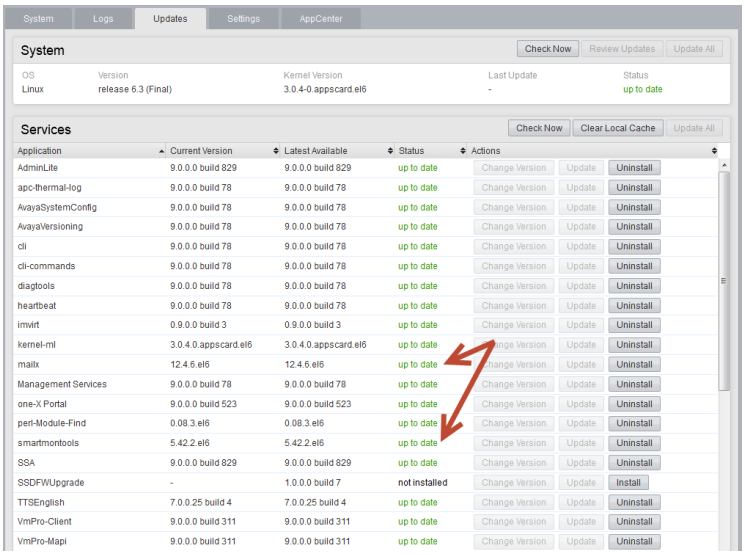

Figure 7

4. Upon successful completion of the SSD Firmware Upgrade package the UCM will automatically power down. For cases where the SSD Firmware Upgrade is not required the installation of the .rpm files will not effect the system and the UCM will not shut down.
5. The UCM can be restarted via the System Status Application (SSA) (see figure 14) or by pressing the top button on the UCM module.
6. **If the mailx.rpm and the smartmontools.rpm show that they are 'Not Installed' then you must perform the steps below to correct the corrupted .rpm files on the UCM (see Figure 8)**

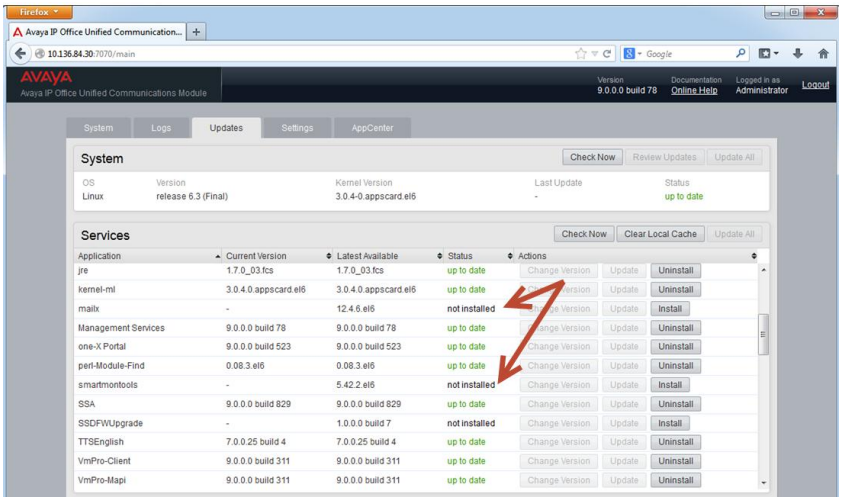

Figure 8

7. If you attempt to install the mailx and smartmontools from the 'Updates' page you will get a Request Error stating the .rpm file is corrupted. (See Figure 9)

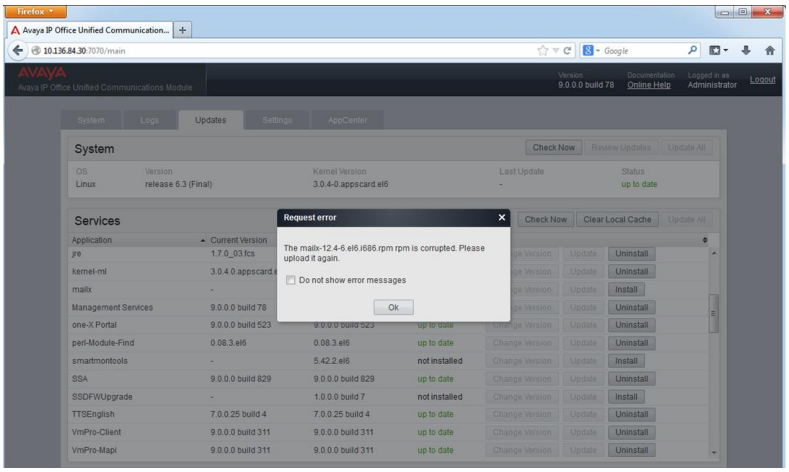

Figure 9

If the mailx.rpm and smartmontools.rpm have been corrupted they can be reloaded to correct the issue. To reload the mailx and smartmontools .rpm files you will need:

a. SSH Client (example, PuTTY www.putty.org).
b. Administrator and root access to the UCM.
c. WebControl access to the UCM.

8. After downloading the PuTTY client you will need to setup PuTTY to access the UCM.
    a. Use the UCM's IP Address in the IP address field.
    b. The Port should be 22.
    c. The connection type should be SSH.

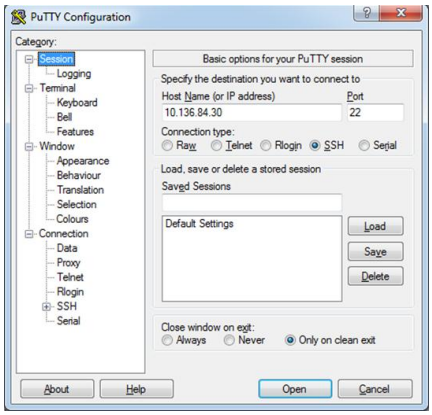

Figure 10

9. Press 'Yes' if you get the 'PuTTY Security Alert'. This alert is displayed every time the PuTTY client is trying to access a new system. (see Figure 11)

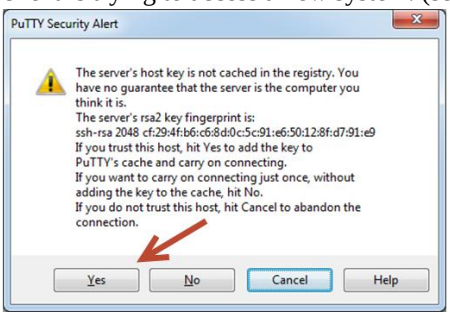

Figure 11

10. Sign-in into the root access on the UCM. Please note that you will need to sign-in as admin after you log-in as the Administrator and before signing in as root. (see Figure 12)

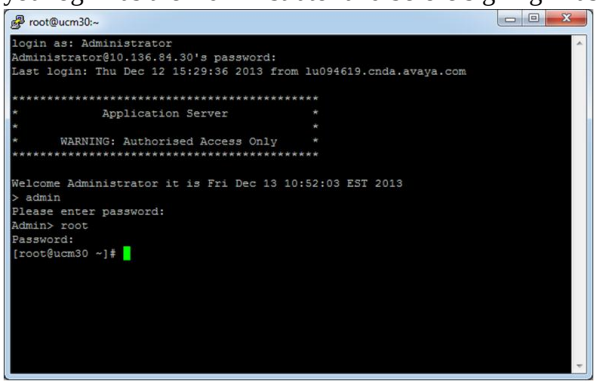

Figure12

11. Type the following command (without the ‘) ‘rpm –import /etc/pki/rpm-gpg/*’ (see Figure 13)

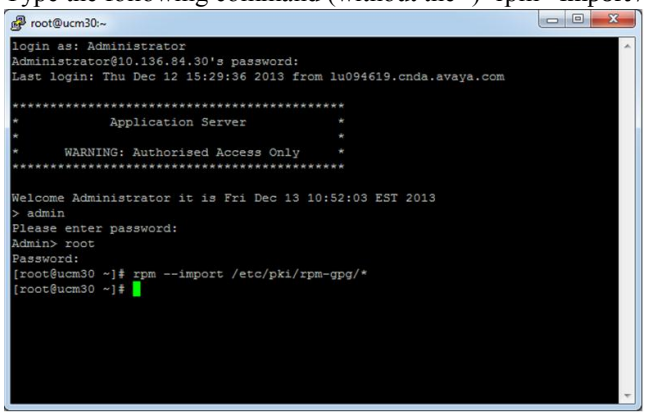

Figure 13

12. Close PuTTy by pressing ‘X’ button.
13. In WebControl ‘Upgrades’ Tab, install ‘mailx’, ‘smartmontools’ and ‘SSDFWUpgrade services in that order. You do not need to reload the zip file.
14. Upon successful completion of the SSD Firmware Upgrade package the UCM will automatically power down. For cases where the SSD Firmware Upgrade is not required the installation of the .rpm files will not effect the system and the UCM will not shut down.
15. The UCM can be restarted via the System Status Application (SSA) (see figure 14) or by pressing the top button on the UCM module.

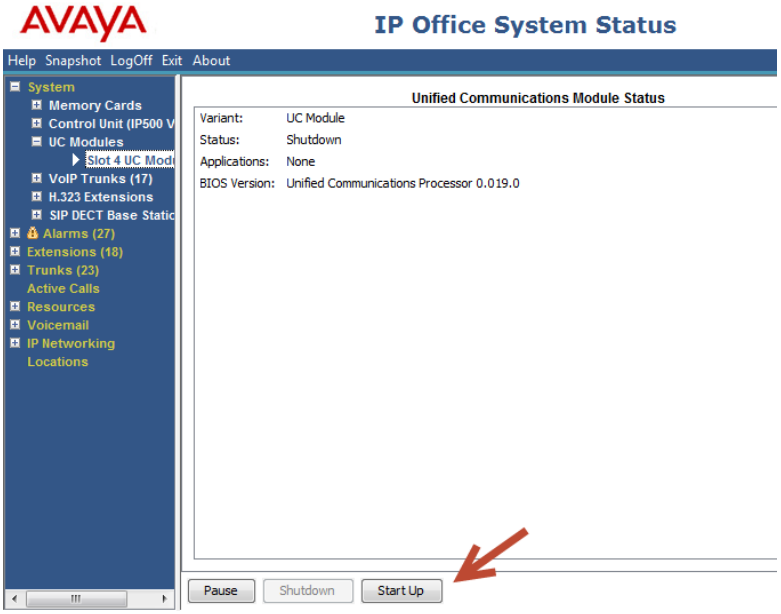

Figure 14

16. Once the UCM has completed the start-up process the diagnostic information will be displayed in the System Status Application (SSA) (see figure 15).

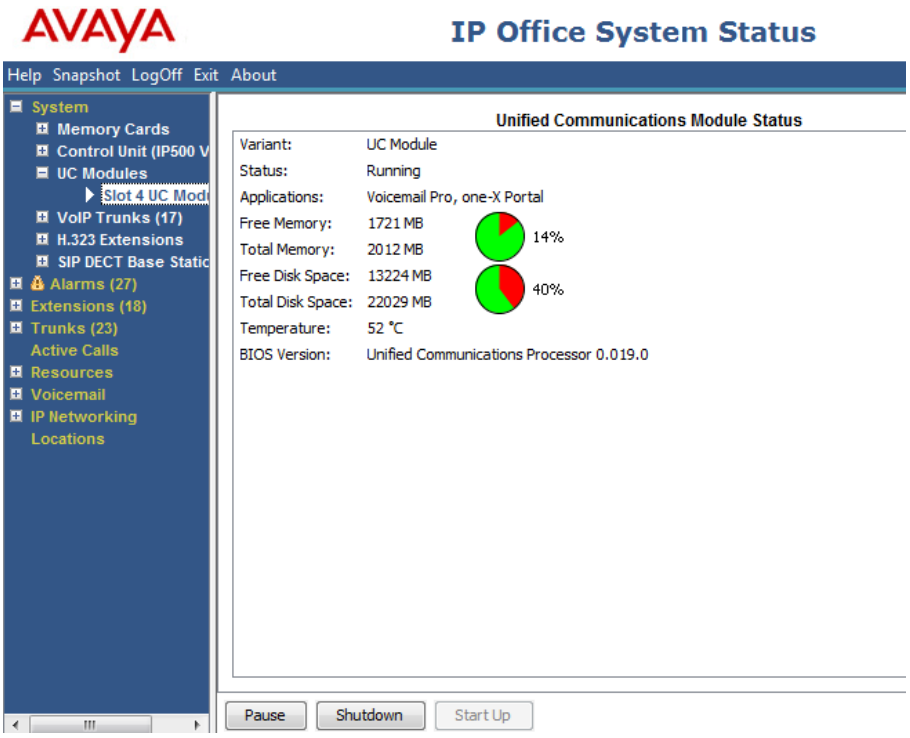

Figure 15

17. The success of the SSD Firmware package can be confirmed by viewing the 'Notifications' window on the WebControl Applications 'Home' tab. This will show four possible messages depending on the SSD version that is installed in the UCM.
    a. 'SSD Firmware not needed. SSD version is Ver703.o'.
    b. 'SSD Firmware not needed. SSD version is S5FAR031'.
    c. 'SSD Firware upgrade successful. Power cycle was completed to finalize the changes'.
    d. 'SSD Firmware upgrade failed'. **In this case, the UCM should be replaced.**
18. The Unified Communications Module (UCM) SSD Firmware Upgrade has been completed.

Verification

FAQ's about the SSD Firmware Package Upgrade

1. What can happen if I choose not to install the SSD Firmware Package Upgrade?
    a. **This corrective action should be performed on all Unified Communications Modules that meet the serial number and PCS level prerequisites. Failure to perform this corrective action will leave the UCM vulnerable to incorrectly lock into a 'write protect' (WP) mode and cause the Preferred Edition Voicemail to shut down. There is a possible risk of data loss if the unit goes into WP mode and this procedure is not performed.**
2. How long does the SSD Firmware Package Upgrade take to complete?
    a. On most drives the upgrade takes less than 3 minutes to complete.
3. Is the SSD Firmware Package Upgrade service effecting?
    a. Yes but only to the Unified Communications Module itself. The Voicemail Pro and the one-X Portal applications will have to be restarted. After the SSD Firmware Package completes the UCM will power down and will have to be restarted either from the System Status Application (SSA) or manually pressing the top button on the UCM Module. All other call processing continues during the SSD Firmware upgrade and the IP500v2 does NOT require a reboot to take effect.
4. My UCM is installed in an active IP500v2 and I cannot take the system down to check and see if the UCM meets the serial number and PCS prerequisites. Should I attempt to install the SSD Firmware Upgrade package anyway?
    a. Yes. The script will determine if the SSD Firmware Upgrade is needed. **For cases where the upgrade is not required, the attempted installation of this upgrade package does not affect the system.**
5. Can I use the upgrade.zip file instead of the full installation image (.iso) file to upgrade my UCM from 8.0 to either 8.1 or 9.0 or from 8.1 to 9.0?
    a. No. You must use the full installation image (.iso) and the USB Initiator method to upgrade between major releases. The upgrade.zip file can only be used to upgrade within the same release. For example, you can use the upgrade.zip file to upgrade from 8.1(x) to 8.1(y).

Failure

n/a

Patch uninstall instructions

n/a

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks

n/a

Avaya Security Vulnerability Classification

Not Susceptible

Mitigation

n/a

If you require further information or assistance please contact your Authorized Service Provider, or visit support.avaya.com. There you can access more product information, chat with an Agent, or open an online Service Request. Support is provided per your warranty or service contract terms unless otherwise specified in the Avaya support Terms of Use.