Product Support Notice

PSN #	PSN005021u

Original publication date: 19 June 2017. This is Issue #01, published date: 19 June 2017.

Severity/risk level	High	Urgency	Immediately

Name of problem

Remote unauthorized file access on Avaya IP Office

Products affected

Avaya IP Office™ Server Edition (native and virtual server), Linux Application Server (native and virtual server), and UCM v1/v2
Releases:
10.1.0.0.x
10.0.0.0.x
10.0.0.1.x
10.0.0.2.x
10.0.0.3.x
10.0.0.4.x
9.1.0.0.x
9.1.0.1.x
9.1.0.2.x
9.1.0.3.x
9.1.0.4.x

Powered by Avaya IP Office™ Releases:
1.x
2.0

Problem description

A web services component of UCMv1/v2, Server Edition, and Linux Application servers could potentially be compromised by a remote unauthorized user.

This remote unauthorized user could upload and download files to the server.

Resolution

If Release 10.0 or Release 10.1: Install the IP Office critical patch detailed below.

If Release 9.1: Upgrade to the latest R9.1 service pack. No patch installation is required.

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

n/a

Download

Check which version of IP Office is currently installed:

1. Log into the server's Web Control Panel (https://<ip-address>:7071/login) using the Administrator account.
   The version is displayed at the top of the screen.
2. Download and install the patch as given below if one of the following versions is installed:
   10.0.0.0.x
   10.0.0.1.x
   10.0.0.2.x
   10.0.0.3.x
   10.0.0.4.x
   10.1.0.0.x

3. Upgrade to the latest R9.1 service pack if one of the following versions is installed:
   9.1.0.0.x
   9.1.0.1.x
   9.1.0.2.x
   9.1.0.3.x
   9.1.0.4.x
   No patch installation is required.

Download of the patch for Release 10.0 and 10.1:

1. To download the IP Office patch, there are two options: Avaya Support site or PLDS. The patch is the same for all IP Office R10.0 and R10.1 Linux components.
   A. To download from the Ayava Support site:

a. Go to Avaya Support (http://support.avaya.com).
b. Click **Support by Products** > **Downloads**:
c. In **Enter Product Name**, type `IP Office`.
d. In Choose Release, select the appropriate release from the drop-down menu.
e. In the list of Downloads, locate and select the appropriate download titled 'IP Office R10/R10.1 Critical Web Service Update' (paging might be necessary to find the entry).

   B. To download from PLDS:

f. Go to the link- https://plds.avaya.com.
a. Enter your login ID and password. You may have to search for and enter your company name or accept the one time EULA or both to gain access to software download.
b. Select **View Downloads**.
c. In the **Search by Download** tab, enter the correct PLDS ID (see the table below) in the **Download pub ID search** field and select **Search Downloads**.
d. Click the Download link to begin the download.

IP Office 10.0:

PLDS ID	IPO00000716
File Name	webservice-patch-10_0-10_1.zip
MD5 Sum	83f061742a0beaccb5202565eafb4af7

IP Office 10.1:

PLDS ID	IPO00000716
File Name	webservice-patch-10_0-10_1.zip
MD5 Sum	83f061742a0beaccb5202565eafb4af7

2. Before you start installing the patch, check the md5 checksum of the file by running the following command from the command line:
   `md5sum webservice-patch-10_0-10_1.zip`
3. If the MD5 checksum does not match the stated value, do not proceed with installation. Download the patch again and verify the MD5 checksum matches.
4. If the MD5 checksum matches, unzip the files to a local directory of the browser PC:
   - apache-tomcat-7.0.55-32.noarch.rpm
   - apache-tomcat-7.0.55-32.noarch.md5.txt – MD5 checksum of rpm
   - README-apache-tomcat-7.0.55-32.noarch.txt
5. Using a text file viewer, read `README-apache-tomcat-7.0.55-32.noarch.txt` for additional information before proceeding with patch installation.

Patch install instructions	Service-interrupting?
1. Installation of the patch will cause the Web Manager, WebLM, and Media Manager applications to restart. Before proceeding, ensure that no undesirable service interruption will occur.	Yes
2. Log into the server's Web Control Panel (https://<ip-address>:7071/login) by using the Administrator account.	
3. Go to **Settings > General > Software Repositories > Application**, and click **Local**.	

4. Click **Browse** and find the apache-tomcat-7.0.55-32.noarch.rpm.
5. Click **Add**. Wait for the upload to finish.
6. Go to **Updates > Services** and find the apache-tomcat application and click **Update**.
   The system restarts Web Manager, Web License Manager, and Media Manager (R10.1 only) applications.

Verification

1. Check **Updates > Services** for the apache-tomcat application Current Version, which should indicate '7.0.0.1.55 build 32'.
2. In **System > Services**, check that the Web Manager service is running.
3. If configured to start automatically, check that the Web License Manager and Media Manager (R10.1 only) services are running.

Failure

Contact Technical Support.

Patch uninstall instructions

The patch cannot be uninstalled.

Security Notes

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

Security risks

A remote unauthorized user could upload and download files to the server.

Avaya Security Vulnerability Classification

High

Mitigation

If Release 10.0 or Release 10.1: Install the IP Office critical patch described above.

If Release 9.1: Upgrade to the latest R9.1 service pack.

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.