



---

**Avaya IP Office™ Platform Patches to address  
Apache Log4j Vulnerability for release 11.0  
Feature Pack 4 Service Pack 6 (11.0.4.6)**

Issue 002



## 1 Contents

1	Contents.....	2
2	Document changes .....	3
3	Introduction .....	3
4	Important Information.....	3
5	Critical Patch deployment instructions for Avaya IP Office 11.0 Feature Pack 4 Service Pack 6 (R11.0.4.6).....	3



## 2 Document changes

Date	Description
17 <sup>th</sup> Dec, 2021	Document issued.
20 <sup>th</sup> Dec, 2021	Support for UCM V1/V2 added.

## 3 Introduction

Avaya is releasing the critical patch to address the Apache Log4J vulnerability CVE-2021-44228 for the Avaya IP Office™ Platform release 11.0 Feature Pack 4 Service Pack 6 (11.0.4.6) which was highlighted in the PSN [PSN005946u-IP Office Log4j vulnerability \(CVE-2021-44228\) \(avaya.com\)](#)

## 4 Important Information

**This critical patch is available on Avaya IP Office 11.0 Feature Pack 4 Service Pack 6 (R11.0.4.6) only, so any customer must first upgrade their IP Office systems to the GA version of this release.**

**The critical patch can be found on the IP Office release 11.0 Feature Pack 4 Service Pack 6 download page on [support.avaya.com](http://support.avaya.com).**

## 5 Critical Patch deployment instructions for Avaya IP Office 11.0 Feature Pack 4 Service Pack 6 (R11.0.4.6).

To close the vulnerability in R11.0.4.6, the one-X portal service needs to apply the provided critical patch which will address the one-X, Web RTC Gateway and Web Collaboration services.

To close the vulnerability, as per the mitigation steps ([Log4j – Apache Log4j Security Vulnerabilities](#)) provided by the Apache, JndiLookup class is removed from the log4j V2.12.1 libraries used in the applications.

Please apply patch to every IP Office server running any of the vulnerable applications.

The critical patch for R11.0.4.6 contains the following artifacts:

Component	Artifact
one-X portal RPM for Linux platform.	oneXportal-11.0.4601-34.rpm
one-X portal installation for Microsoft Windows Server	onexportal_11.0.4601.34.zip

### Deploying critical patch on Server Edition and Application Server

1. Login to Web control Panel.
2. Navigate to the 'Settings->General' and upload the RPM using 'Applications' options.
3. Navigate to the 'Updates' tab.



4. Apply the patch to 'one-X Portal' Service.
5. Verify the version in services tab of Web Control Panel matches the artifact version.

#### **Deploying critical patch on UCM V1/V2**

1. Login to Web control Panel.
2. Stop the one-X Portal service from System->Services'.
3. Navigate to the 'Settings->General' and upload the RPM using 'Applications' options.
4. Navigate to the 'Updates' tab.
5. Apply the patch to 'one-X Portal' Service.
6. Verify the version in services tab of Web Control Panel matches the artifact version.
7. Start the one-X Portal service from System->Services'.

#### **Deploying critical patch on Windows platform.**

1. Extract the onexportal\_11.0.4601.34.zip on to the windows machine running one-X Portal server.
2. Run setup.exe and perform the suggested upgrade steps.
3. Verify the version of one-X Portal matches the artifact version.