Product Support Notice

PSN #	PSN005385u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: 1st April 2019 This is Issue #01, published date: 1st April 2019.	Severity/risk level	Critical	Urgency	Immediately

Name of problem

Release of IP Office Contact Center 10.1.2.2.5-11204.1908- Patch

Products affected

This issue affects IP Office Contact Center **9.x, 10.0.x, 10.1.2.x**

Thin Client/Web UI - ONLY

Problem description

A SQL injection vulnerability in the WebUI component of IP Office Contact Center could allow an authenticated attacker to retrieve or alter sensitive data related to other users on the system. Affected versions of IP Office Contact Center include all 9.x &10.x versions prior to IPOCC10.1.2.2.5-11204.1908. Unsupported versions not listed here were not evaluated.

This issue has been assigned CVE-2019-7001.

CVSS RISK/SCORE:

CRITICAL, 9.9 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)

PROBLEM TYPE:

CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Resolution

Download and apply IPOCC 10.1.2.2.5-11204.1908.

This software is available as a download by Avaya Associates via PLDS from http://support.avaya.com/download

To download the patch:

Go to http://support.avaya.com and select product as **IP Office Contact Center** and select the release version as **10.1.x**

Here is a direct link: https://support.avaya.com/downloads/download-details.action?contentId=C2019241625456940_4&productId=P1568&releaseId=10.1.x

Important: Customers on **IPOCC 9.x/10.x** versions **should upgrade to the latest 10.1.2.x** and then apply the patch.

Note: It is recommended that you go sequential in terms of upgrading. Example: 9.x to 10.1 and then to 10.1.2.x

Workaround or alternative remediation*

If the WebUI and the Webservices are not required by the customer, please proceed as followed:

Under “C:\Program Files (x86)\Avaya\IP Office Contact Center\Tomcat WWW\webapps” delete the following folders:

…\DirectoryWS

….\ WebUI

Restart the IPOCC Server

Note: Even if a user is just an IPOCC UI user, they are still a valid user for the WebUI

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	
Downloaded ZIP file contains the backup instructions in a Readme.txt file.	
Download	
Refer to Resolution section for download details	
Patch install instructions	**Service-interrupting?**
Downloaded ZIP file contains the patch install instructions in a Readme.txt file	Yes
Verification	
Downloaded ZIP file contains the patch verification instructions in a Readme.txt file	
Failure	
Contact Technical Support	
Patch uninstall instructions	
Downloaded ZIP file contains the patch uninstall instructions in a Readme.txt file.	

Security Notes

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

Security risks
Data compromise with SQL injection
Avaya Security Vulnerability Classification
Critical
Mitigation
Apply this immediately.

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.