Product Support Notice

PSN # PSN006198u

Original publication date: 16-June-2023. This is Issue #01, published date: 16-June-2023. Severity/risk level High Urgency Immediately

Name of problem

IP Office Release 11.1.3.0 Server Edition (Cent OS 7 based software)

Products affected

IPO Server Edition 11.1.3.0

Problem description

IP Office 11.1.3 is a minor software release with the following corrective content and minor enhancements. The details of the features will be listed in the Tech Bulletin and documentation issued along with the 11.1.3 release. (Planned GA date 27th June 2023)

–Workplace Auto-Answer

–Self Contact Avatar

–46xxspecials.txt

–CEC Updates (cert levels)

–Hardware obsolescence (PRI/VCM)

IP Office 11.1.3.0 will contain only the following vulnerability fixes:

- WebManager and Webcontrol - Web Manager security response returned plain-text from the application
- WebManager and Webcontrol Platform and Software Versions Revealed - The server software versions used by the application are revealed by the web server.
- External researcher Authenticated user file intervention - one-X portal File upload Vulnerability

Any future 11.1.3.x service packs will only contain bug fixes from Customer Found Defects (CFDs). There will not be any additional CVE/vulnerability updates. Any further CVE's and vulnerabilities will only be addressed in IP Office 12.0.

IP Office 12.0 will be based on Rocky Linux and will include regular CVE/vulnerability updates identified in RLSAs (Rocky Linux Security Advisories) for robust security protection.

Solutions

Remarks

None

Software Update Notes

The information in this section concerns a new software package, recommended in the Resolution above.

Backup before applying the software package

n/a

Download

n/a

Software install instructions	Service-interrupting?
n/a	No

Verification
n/a

Failure
n/a

Software 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.