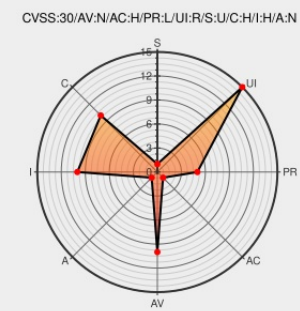
CVE-2019-7004

Published on: 12/11/2019 12:00:00 AM UTC

Last Modified on: 02/02/2023 02:24:00 AM UTC

CVE-2019-7004 - advisory for ASA-2019-213

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ip Office Application Server from Avaya contain the following vulnerability:

A Cross-Site Scripting (XSS) vulnerability in the WebUI component of IP Office Application Server could allow unauthorized code execution and potentially disclose sensitive information. All product versions 11.x are affected. Product versions prior to 11.0, including unsupported versions, were not evaluated.

CVE-2019-7004 has been assigned by securityalerts@avaya.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Avaya** - **IP Office Application Server** version **11.0 FP4 SP1**

CVSS3 Score: 5.4 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVSS2 Score: 3.5 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Avaya IP Office Application Server 11.0.0.0	packetstormsecurity.com	MISC packetstormsecurity.com/files/156476/Avaya-IP-

Cross Site Scripting ≈ Packet Storm	text/html	Office-Application-Server-11.0.0.0-Cross-Site-Scripting.html
ASA-2019-213	Vendor Advisory support.avaya.com text/html	CONFIRM support.avaya.com/css/P8/documents/101062833

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Avaya	Ip Office Application Server	All	All	All	All

cpe:2.3:a:avaya:ip_office_application_server:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→