



CVE-2019-16970

Published on: 10/21/2019 12:00:00 AM UTC

Last Modified on: 02/03/2023 09:34:00 PM UTC

CVE-2019-16970

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Fusionpbx](#) from [Fusionpbx](#) contain the following vulnerability:

In FusionPBX up to 4.5.7, the file `app\sip_status\sip_status.php` uses an unsanitized "savemsg" variable coming from the URL, which is reflected in HTML, leading to XSS.

CVE-2019-16970 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
FusionPBX XSS 3 – Resp3ct blog	Third Party Advisory resp3ctblog.wordpress.com text/html	MISC resp3ctblog.wordpress.com/2019/10/19/fusionpbx-xss-3/
Update sip_status.php ·	Patch	MISC

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	Fusionpbx	Fusionpbx	All	All	All	All
cpe:2.3:a:fusionpbx:fusionpbx:*****:*****:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→