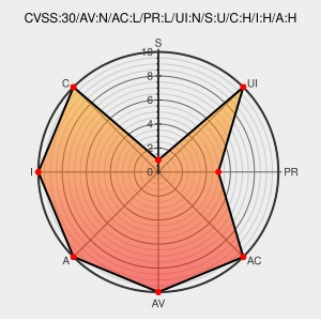
CVE-2019-15029

Published on: 09/05/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:44 PM UTC

CVE-2019-15029

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



Certain versions of Fusionpbx from Fusionpbx contain the following vulnerability:

FusionPBX 4.4.8 allows an attacker to execute arbitrary system commands by submitting a malicious command to the service_edit.php file (which will insert the malicious command into the database). To trigger the command, one needs to call the services.php file via a GET request with the service id followed by the parameter a=start to execute the stored command.

CVE-2019-15029 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
FusionPBX-exploit.py · GitHub	Exploit Third Party Advisory	MISC gist.github.com/mhaskar/7a6a804cd68c7fec4f9d1f5c3507900f

	gist.github.com text/html	
FusionPBX v4.4.8 authenticated Remote Code Execution (CVE-2019-15029) - Shells.Systems	Exploit Third Party Advisory shells.systems text/html	MISC shells.systems/fusionpbx-v4-4-8-authenticated-remote-code-execution-cve-2019-15029/
FreePBX-exploit.mp4 - Google Drive	Exploit Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC drive.google.com/file/d/1bt08NSUaxu87LJJGdNd7LpvZ2uGauRK8/view?usp=sharing

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

Exploit/POC from Github

The official exploit code for FusionPBX v4.4.8 Remote Code Execution CVE-2019-15029

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fusionpbx	Fusionpbx	4.4.8	All	All	All
Application	Fusionpbx	Fusionpbx	4.4.8	All	All	All

cpe:2.3:a:fusionpbx:fusionpbx:4.4.8:*:*:*:*:*:*:*:

cpe:2.3:a:fusionpbx:fusionpbx:4.4.8:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→