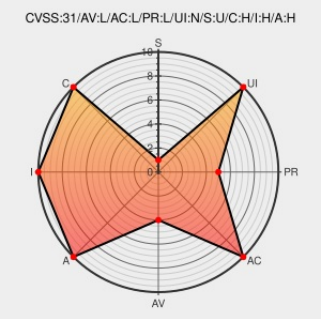
CVE-2018-16156

Published on: 05/17/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:34 PM UTC

CVE-2018-16156

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



Certain versions of Paperstream Ip Twain from Fujitsu contain the following vulnerability:

In PaperStream IP (TWAIN) 1.42.0.5685 (Service Update 7), the FJTWSVIC service running with SYSTEM privilege processes unauthenticated messages received over the FjtwMkic_Fjicube_32 named pipe. One of these message processing functions attempts to dynamically load the UninOldIS.dll library and executes an exported function named ChangeUninstallString. The default install does not contain this library and therefore if any DLL with that name exists in any directory listed in the PATH variable, it can be used to escalate to SYSTEM level privilege.

CVE-2018-16156 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link

CVE-2018-16156 – Securifera	Third Party Advisory www.securifera.com text/html	MISC www.securifera.com/advisories/cve-2018-16156/
PaperStream IP (TWAIN) 1.42.0.5685 Local Privilege Escalation ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/160832/PaperStream-IP-TWAIN-1.42.0.5685-Local-Privilege-Escalation.html

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	Fujitsu	Paperstream Ip Twain	1.42.0.5685	All	All	All
Application	Fujitsu	Paperstream Ip Twain	1.42.0.5685	All	All	All
Application	Fujitsu	Paperstream Ip Twain	1.42.0.5685	All	All	All

cpe:2.3:a:fujitsu:paperstream_ip_(twain):1.42.0.5685:*:*:*:*:*:*:*:

cpe:2.3:a:fujitsu:paperstream_ip_\(twain\):1.42.0.5685:*:*:*:*:*:*:*:

cpe:2.3:a:fujitsu:paperstream_ip_\(twain\):1.42.0.5685:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→