



CVE-2017-13771

Published on: 09/07/2017 12:00:00 AM UTC

Last Modified on: 07/20/2021 05:15:00 PM UTC

CVE-2017-13771

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

Certain versions of [Scan To Network](#) from [Lexmark](#) contain the following vulnerability:

Lexmark Scan To Network (SNF) 3.2.9 and earlier stores network configuration credentials in plaintext and transmits them in requests, which allows remote attackers to obtain sensitive information via requests to (1) `cgi-bin/direct/printer/ptappauth/apps/snfDestServlet` or (2) `cgi-bin/direct/printer/ptappauth/apps/ImportExportServlet`.

CVE-2017-13771 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
Lexmark Security Advisories	support.lexmark.com text/html	MISC support.lexmark.com/alerts
Full Disclosure: Lexmark Scan to Network (SNF) printer	Exploit	FULL DISC: 20170831 Lexmark Scan to Network

Full Disclosure: Lexmark Scan To Network (SNF) printer application <= 3.2.9 Information Exposure	Exploit Mailing List Third Party Advisory seclists.org text/html	Full Disclosure: Lexmark Scan To Network (SNF) printer application <= 3.2.9 Information Exposure
Lexmark Scan To Network (SNF) 3.2.9 Information Disclosure ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/143975/Lexmark-Scan-To-Network-SNF-3.2.9-Information-Disclosure.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	Lexmark	Scan To Network	All	All	All	All
cpe:2.3:a:lexmark:scan_to_network:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)