



Published on: 10/18/2014 12:00:00 AM UTC

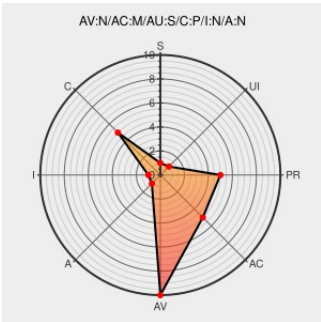
Last Modified on: 03/23/2021 11:25:52 PM UTC

CVE-2014-5420

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of **Pyxis Supplystation** from **Carefusion** contain the following vulnerability:

CareFusion Pyxis SupplyStation 8.1 with hardware test tool before 1.0.16 has a hardcoded application password, which makes it easier for remote authenticated users to obtain application-file access via unspecified vectors.

CVE-2014-5420 has been assigned by  ics-cert@hq.dhs.gov to track the vulnerability

CVSS2 Score: 3.5 - LOW

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

CVE References

Description	Tags	Link
CareFusion Pyxis SupplyStation System Vulnerabilities ICS-CERT	US Government Resource ics-cert.us-cert.gov text/html	 MISC ics-cert.us-cert.gov/advisories/ICSA-14-288-01

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
Hardware 	Carefusion	Pyxis Supplystation	8.1	All	All	All
Hardware 	Carefusion	Pyxis Supplystation	8.1	All	All	All
cpe:2.3:h:carefusion:pyxis_supplystation:8.1:*****:						
cpe:2.3:h:carefusion:pyxis_supplystation:8.1:*****:						
No vendor comments have been submitted for this CVE						
← Previous ID			Next ID→			