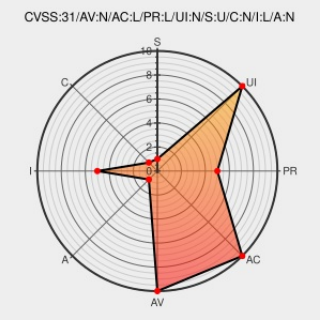
CVE-2020-9013

Published on: 02/16/2020 12:00:00 AM UTC

Last Modified on: 01/01/2022 07:53:00 PM UTC

CVE-2020-9013

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



Certain versions of Skillpipe from Arvato contain the following vulnerability:

Arvato Skillpipe 3.0 allows attackers to bypass intended print restrictions by deleting from the HTML source code.

CVE-2020-9013 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 4.3 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
Skillpipe - Remove the Watermark (Course Reader used by Microsoft) using Ad Blocking [CVE-2020-9013] - YouTube	Third Party Advisory www.youtube.com text/html	MISC www.youtube.com/watch?v=Ok1UmRFWoLY

Gerard Fuguet Morales on Twitter: "In 2017 I reported a vulnerability in #skillpipe that let you strip the watermark from #MOC. At present, #Microsoft students can achieve it plus #AdblockPlus to "Semi-Automate" the hacking process #BeGoodBeHackers #InfoSec #CyberSecurity https://t.co/rvncrEkzL0"	Third Party Advisory nitter.domain.glass text/html	MISC twitter.com/GerardFuguet/status/1228462263188758529
	www.exploit-db.com Proof of Concept application/pdf	MISC www.exploit-db.com/docs/48175

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	Arvato	Skillpipe	3.0	All	All	All
Application	Arvato	Skillpipe	3.0	All	All	All

cpe:2.3:a:arvato:skillpipe:3.0:*:*:*:*:*:*:*:

cpe:2.3:a:arvato:skillpipe:3.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→

© CVE.report 2023 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report