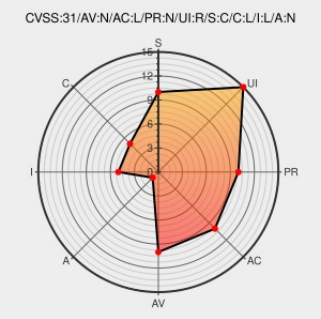
CVE-2020-29456

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

Last Modified on: 03/23/2021 11:24:10 PM UTC

CVE-2020-29456

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



Certain versions of Papermerge from Papermerge contain the following vulnerability:

Multiple cross-site scripting (XSS) vulnerabilities in Papermerge before 1.5.2 allow remote attackers to inject arbitrary web script or HTML via the rename, tag, upload, or create folder function. The payload can be in a folder, a tag, or a document's filename. If email consumption is configured in Papermerge, a malicious document can be sent by email and is automatically uploaded into the Papermerge web application. Therefore, no authentication is required to exploit XSS if email consumption is configured. Otherwise authentication is required.

CVE-2020-29456 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.1 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link

Open Source - Papermerge - Document Management System	Product www.papermerge.com text/html	MISC www.papermerge.com/
Stored Cross-Site Scripting (XSS) · Issue #228 · ciur/papermerge · GitHub	Third Party Advisory github.com text/html	MISC github.com/ciur/papermerge/issues/228
Release Version 1.5.2 · ciur/papermerge · GitHub	Release Notes Third Party Advisory github.com text/html	MISC github.com/ciur/papermerge/releases/tag/v1.5.2

Related QID Numbers

982732 Python (pip) Security Update for papermerge (GHSA-9w49-m7xh-5r39)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Papermerge	Papermerge	All	All	All	All
Application	Papermerge	Papermerge	All	All	All	All

cpe:2.3:a:papermerge:papermerge:*:*:*:*:*:*:*:*:

cpe:2.3:a:papermerge:papermerge:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→