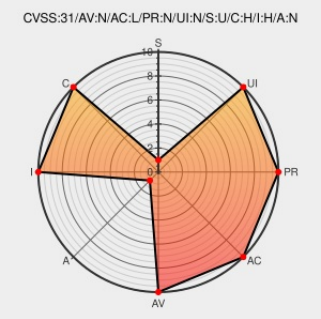
CVE-2022-24840

Published on: Not Yet Published

Last Modified on: 06/17/2022 03:50:00 PM UTC

CVE-2022-24840 - advisory for GHSA-4w8f-hjm9-xwgf

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



Certain versions of Django-s3file from Django-s3file Project contain the following vulnerability:

django-s3file is a lightweight file upload input for Django and Amazon S3 . In versions prior to 5.5.1 it was possible to traverse the entire AWS S3 bucket and in most cases to access or delete files. If the `AWS_LOCATION` setting was set, traversal was limited to that location only. The issue was discovered by the maintainer. There were no reports of the vulnerability being known to or exploited by a third party, prior to the release of the patch. The vulnerability has been fixed in version 5.5.1 and above. There is no feasible workaround. We must urge all users to immediately updated to a patched version.

CVE-2022-24840 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **codingjoe** - **django-s3file** version **< 5.5.1**

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: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Fix CVE-XXXX-XXXX -- Fix Path Traversal security vulnerability · codingjoe/django-s3file@68ccd2c · GitHub	github.com text/html	MISC github.com/codingjoe/django-s3file/commit/68ccd2c621a40eb66fdd6af2be9d5fcc9c373318
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') in django-s3file · Advisory · codingjoe/django-s3file · GitHub	github.com text/html	CONFIRM github.com/codingjoe/django-s3file/security/advisories/GHSA-4w8f-hjm9-xwgf

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Django-s3file Project	Django-s3file	All	All	All	All

cpe:2.3:a:django-s3file_project:django-s3file:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-24840 : django-s3file is a lightweight file upload input for Django and Amazon S3 . In versions prior to 5… twitter.com/i/web/status/1…	2022-06-09 04:08:15
/r/netcve	CVE-2022-24840	2022-06-09 05:38:23

← Previous ID

Next ID→