



CVE-2022-42731

Published on: Not Yet Published

Last Modified on: 10/11/2022 07:05:00 PM UTC

CVE-2022-42731

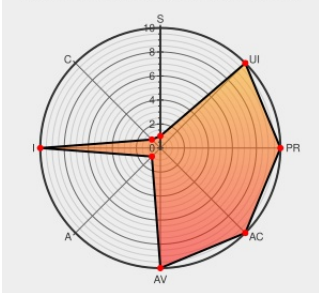
Source: Mitre

Source: NIST

CVE.ORG

Print: PDF

CVSS:31/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N



Certain versions of [Django-mfa2](#) from [Django-mfa2 Project](#) contain the following vulnerability:

mfa/FIDO2.py in django-mfa2 before 2.5.1 and 2.6.x before 2.6.1 allows a replay attack that could be used to register another device for a user. The device registration challenge is not invalidated after usage.

CVE-2022-42731 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
Release v2.5.1 - Security Updated · mkalioby/django-mfa2 · GitHub	github.com text/html	MISC github.com/mkalioby/django-mfa2/releases/tag/v2.5.1-release
django-mfa2/FIDO2.py at 0936ea253354dd95cb127f09d0efa31324caef27 · mkalioby/django-mfa2 · GitHub	github.com text/html	MISC github.com/mkalioby/django-mfa2/blob/0936ea253354dd95cb127f09d0efa31324caef27/mfa/FIDO2.py#L5
Release v2.6.1 - Security Update · mkalioby/django-mfa2 · GitHub	github.com text/html	MISC github.com/mkalioby/django-mfa2/releases/tag/v2.6.1-release

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

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Django-mfa2 Project	Django-mfa2	All	All	All	All
cpe:2.3:a:django-mfa2_project:django-mfa2:*:*:*:*:*.*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-42731 : mfa/FIDO2.py in django-mfa2 before 2.5.1 and 2.6.x before 2.6.1 allows a replay attack that could... twitter.com/i/web/status/1...	2022-10-11 14:07:28
 @Inceptus3	New Vulnerability: CVE-2022-42731 #InceptusSecure #UnderOurProtection	2022-10-11 16:19:31
 /r/netcve	CVE-2022-42731	2022-10-11 14:38:40

[← 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 registered 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](#)