



CVE-2023-25575

Published on: Not Yet Published

Last Modified on: 03/13/2023 04:05:00 PM UTC

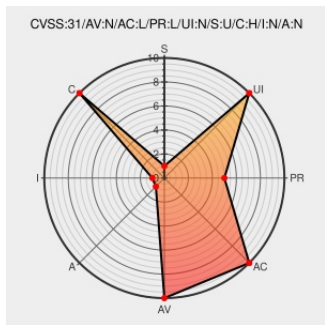
CVE-2023-25575 - advisory for GHSA-vr2x-7687-h6qv

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of **Core** from **Api-platform** contain the following vulnerability:

API Platform Core is the server component of API Platform: hypermedia and GraphQL APIs. Resource properties secured with the `security` option of the `ApiPlatform\Metadata\ApiProperty` attribute can be disclosed to unauthorized users. The problem affects most serialization formats, including raw JSON, which is enabled by default

when installing API Platform. Custom serialization formats may also be impacted. Only collection endpoints are affected by the issue, item endpoints are not. The JSON-LD format is not affected by the issue. The result of the security rule is only executed for the first item of the collection. The result of the rule is then cached and reused for the next items. This bug can leak data to unauthorized users when the rule depends on the value of a property of the item. This bug can also hide properties that should be displayed to authorized users. This issue impacts the 2.7, 3.0 and 3.1 branches. Please upgrade to versions 2.7.10, 3.0.12 or 3.1.3. As a workaround, replace the `cache_key` of the context array of the Serializer inside a custom normalizer that works on objects if the security option of the `ApiPlatform\Metadata\ApiProperty` attribute is used.

CVE-2023-25575 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **api-platform** - core version = >= 3.0.0, < 3.0.12

Affected Vendor/Software: **api-platform** - core version = >= 3.1.0, < 3.1.3

Affected Vendor/Software: **api-platform** - core version = >= 2.6.0, < 2.7.10

CVSS3 Score: **6.5 - MEDIUM**

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

Impact

Impact

Impact

UNCHANGED

HIGH

NONE

NONE

CVE References

Description

Tags

Link

Merge pull request from GHSA-vr2x-7687-h6qv · api-platform/core@5723d68 · GitHub

github.com
text/html

MISC github.com/api-platform/core/commit/5723d68369722feefeb11e42528d9580db5dd0fb

Secured properties may be accessible within collections · Advisory · api-platform/core · GitHub

github.com
text/html

MISC github.com/api-platform/core/security/advisories/GHSA-vr2x-7687-h6qv

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	Api-platform	Core	All	All	All	All
cpe:2.3:a:api-platform:core:*:*:*:*:*:*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@s0yuka	An API Platform #security issue got fixed, upgrade now! Details of the CVE-2023-25575 at github.com/api-platform/c..... twitter.com/i/web/status/1...	2023-02-28 10:43:00
@ipssignatures	The vuln CVE-2023-25575 has a tweet created 0 days ago and retweeted 10 times. twitter.com/s0yuka/status/... #pow1rtrtwwcve	2023-02-28 14:06:01
@CVEreport	CVE-2023-25575 : API Platform Core is the server component of API Platform: hypermedia and GraphQL APIs. Resource p... twitter.com/i/web/status/1...	2023-02-28 23:07:42
/r/netcve	CVE-2023-25575	2023-03-01 00:38:43

[← 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