



# Potential exposure of private data due to incorrect handling of Vary: \* in UpdateCacheMiddleware

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#) 

## Summary

<b>CVE</b>	CVE-2026-6907
<b>State</b>	PUBLISHED
<b>Assigner</b>	DSF
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-05 16:16:18 UTC
<b>Updated</b>	2026-05-07 14:16:04 UTC
<b>Description</b>	An issue was discovered in 6.0 before 6.0.5 and 5.2 before 5.2.14. `django.middleware.cache.UpdateCacheMiddleware` er

## Risk And Classification

**Primary CVSS:** v4.0 2.3 LOW from 6a34fbeb-21d4-45e7-8e0a-62b95bc12c92

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**Problem Types:** CWE-524 | CWE-524 CWE-524: Use of Cache Containing Sensitive Information

Version	Source	Type	Score	Severity	Vector
4.0	6a34fbeb-21d4-45e7-8e0a-62b95bc12c92	Secondary	2.3	LOW	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:L/VI:N/V
4.0	CNA	DECLARED	2.3	LOW	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:L/VI:N/V
3.1	nvd@nist.gov	Primary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
3.1	6a34fbeb-21d4-45e7-8e0a-62b95bc12c92	Secondary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N
3.1	CNA	DECLARED	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

None

User Interaction

Passive

Confidentiality

Low

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Djangoproject	Django	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Djangoproject</a>	<a href="#">Django</a>	affected 6.0 6.0.5 python	Not specified
CNA	<a href="#">Djangoproject</a>	<a href="#">Django</a>	unaffected 6.0.5 python	Not specified
CNA	<a href="#">Djangoproject</a>	<a href="#">Django</a>	affected 5.2 5.2.14 python	Not specified
CNA	<a href="#">Djangoproject</a>	<a href="#">Django</a>	unaffected 5.2.14 python	Not specified

## References

Reference	Source	Link	Tags
<a href="https://groups.google.com/g/django-announce">groups.google.com/g/django-announce</a>	6a34fbeb-21d4-45e7-8e0a-62b95bc12c92	<a href="https://groups.google.com">groups.google.com</a>	Third Party
<a href="https://docs.djangoproject.com/en/dev/releases/security">docs.djangoproject.com/en/dev/releases/security</a>	6a34fbeb-21d4-45e7-8e0a-62b95bc12c92	<a href="https://docs.djangoproject.com">docs.djangoproject.com</a>	Vendor
<a href="https://www.djangoproject.com/weblog/2026/may/05/security-releases">www.djangoproject.com/weblog/2026/may/05/security-releases</a>	6a34fbeb-21d4-45e7-8e0a-62b95bc12c92	<a href="https://www.djangoproject.com">www.djangoproject.com</a>	Vendor
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	Canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	Canonical

## Vendor Comments And Credit

### Discovery Credit

**CNA:** Ahmad Sadeddin (en)

**CNA:** Sarah Boyce (en)

**CNA:** Sarah Boyce (en)

## Additional Advisory Data

Source	Time	Event
CNA	2026-03-06T10:17:03.000Z	Initial report received.
CNA	2026-04-23T10:17:26.000Z	Vulnerability confirmed.
CNA	2026-05-05T09:00:00.000Z	Security release issued.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)