Session fixation via public cached pages and SESSION_SAVE_EVERY_REQUEST

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-35192
State	PUBLISHED
Assigner	DSF
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-05 16:16:12 UTC
Updated	2026-05-07 14:20:37 UTC
Description	An issue was discovered in 6.0 before 6.0.5 and 5.2 before 5.2.14. Response headers do not vary on cookies if a session is

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/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-539 | CWE-539 CWE-539: Use of Persistent Cookies 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	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/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/MSC:X/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

Required

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/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	Djangoproject	Django	affected 6.0 6.0.5 python	Not specified

CNA	Djangoproject	Django	unaffected 6.0.5 python	Not specified
CNA	Djangoproject	Django	affected 5.2 5.2.14 python	Not specified
CNA	Djangoproject	Django	unaffected 5.2.14 python	Not specified

References

Reference	Source	Link	Tags
groups.google.com/g/django-announce	6a34fbeb-21d4-45e7-8e0a-62b95bc12c92	groups.google.com	Third
docs.djangoproject.com/en/dev/releases/security	6a34fbeb-21d4-45e7-8e0a-62b95bc12c92	docs.djangoproject.com	Vend
www.djangoproject.com/weblog/2026/may/05/security-releases	6a34fbeb-21d4-45e7-8e0a-62b95bc12c92	www.djangoproject.com	Vend
CVE Program record	CVE.ORG	www.cve.org	canc
NVD vulnerability detail	NVD	nvd.nist.gov	canc

Vendor Comments And Credit

Discovery Credit

CNA: Cantina (en)

CNA: Jake Howard (en)

CNA: Sarah Boyce (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-03-11T10:54:40.000Z	Initial report received.
CNA	2026-04-01T10:54:43.000Z	Vulnerability confirmed.
CNA	2026-05-05T09:00:00.000Z	Security release issued.

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