



BaseCookie.js_output() does not neutralize embedded characters

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

Summary

CVE	CVE-2026-6019
State	PUBLISHED
Assigner	PSF
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-22 20:16:42 UTC
Updated	2026-04-22 21:23:52 UTC
Description	http.cookies.Morsel.js_output() returns an inline <script> snippet and only escapes " for JavaScript string context. It does not

Risk And Classification

Primary CVSS: v4.0 2.1 LOW from cna@python.org

CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:L/VI:L/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-150 | CWE-150 CWE-150 Improper neutralization of escape, meta, or control sequences

Version	Source	Type	Score	Severity	Vector
4.0	cna@python.org	Secondary	2.1	LOW	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:L/VI:L/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
4.0	CNA	CVSS	2.1	LOW	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

High

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:L/VI:L/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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Python Software Foundation	CPython	affected 3.15.0 python	Not specified

References

Reference	Source	Link	Tags
github.com/python/cpython/pull/148848	cna@python.org	github.com	
mail.python.org/archives/list/security-announce@python.org/thread/IVNWGV2BBNC...	cna@python.org	mail.python.org	
github.com/python/cpython/commit/76b3923d688c0efc580658476c5f525ec8735104	cna@python.org	github.com	
github.com/python/cpython/issues/90309	cna@python.org	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

Vendor Comments And Credit

Discovery Credit

CNA: oolongeya (<https://github.com/komi22>) (en)

CNA: Seth Larson (<https://github.com/sethmlarson>) (en)

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

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

CVE.report and Source URL Uptime Status status.cve.report