CVE-2025-65717

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

Summary

CVE	CVE-2025-65717
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-16 16:19:17 UTC
Updated	2026-05-05 18:16:01 UTC
Description	An issue in Visual Studio Code Extensions Live Server v5.7.9 allows attackers to exfiltrate files via user interaction with a cr

Risk And Classification

Primary CVSS: v3.1 4.3 MEDIUM from ADP

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

EPSS: 0.000520000 probability, percentile 0.159620000 (date 2026-05-05)

Problem Types: CWE-79 | CWE-200 | CWE-601 | n/a | CWE-601 CWE-601 URL Redirection to Untrusted Site ('Open Redirect') | CWE-200 CWE-200 Exposure of Sensitive Information to an Unauthorized Actor | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	4.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

Low

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ritwickdey	Live Server	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source	Link	Tags
github.com/ritwickdey/vscode-live-server	cve@mitre.org	github.com	Product
www.ox.security/blog/cve-2025-65717-live-server-vscode-vulnerability	cve@mitre.org	www.ox.security	Exploit, Third Party Adviso
github.com/ritwickdey/vscode-live-server/security/advisories/GHSA-9qrh-5...	cve@mitre.org	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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