



# CVE-2025-1026

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

## Summary

<b>CVE</b>	CVE-2025-1026
<b>State</b>	PUBLISHED
<b>Assigner</b>	snyk
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-02-05 05:15:10 UTC
<b>Updated</b>	2026-04-29 01:00:01 UTC
<b>Description</b>	Versions of the package spatie/browsershot before 5.0.5 are vulnerable to Improper Input Validation due to improper URL v

## Risk And Classification

**Primary CVSS:** v4.0 6.6 MEDIUM from report@snyk.io

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:H/SI:N/SA:N/E:P/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-20 | CWE-20 Improper Input Validation

Version	Source	Type	Score	Severity	Vector
4.0	report@snyk.io	Secondary	6.6	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:H/SI:N/SA:N/E:P/C...
4.0	CNA	DECLARED	7.7	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:H/SI:N/SA:N/E:P
3.1	report@snyk.io	Secondary	8.6	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N
3.1	CNA	DECLARED	8.6	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N/E:P

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

None

Integrity

None

Availability

None

Sub Conf.

High

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:H/SI:N/SA:N/E:P/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

Changed

Confidentiality

High

Integrity

None

Availability

None

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	Spatie/browsershot	affected 5.0.5 semver	Not specified

### References

Reference	Source	Link	Tags
security.snyk.io/vuln/SNYK-PHP-SPATIEBROWSERSHOT-8533024	report@snyk.io	security.snyk.io	
github.com/spatie/browsershot/commit/e3273974506865a24fbb5b65b534d8d4b8d...	report@snyk.io	github.com	

gist.github.com/chuajianshen/6291920112fcf1543fa7b43862112be6	report@snyk.io	<a href="https://gist.github.com">gist.github.com</a>	
github.com/spatie/browsershot/pull/908	report@snyk.io	<a href="https://github.com">github.com</a>	
gist.github.com/mrdgef/54a8783408220c67c1b859df38a52d65	report@snyk.io	<a href="https://gist.github.com">gist.github.com</a>	
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, analysis

## Vendor Comments And Credit

### Discovery Credit

**CNA:** Chua Jian Shen (en)

**CNA:** Ee Yang Tee (en)

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

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/licenses).

**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)