



# HTML injection in PHP Point Of Sale

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

## Summary

<b>CVE</b>	CVE-2025-41011
<b>State</b>	PUBLISHED
<b>Assigner</b>	INCIBE
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-21 16:16:19 UTC
<b>Updated</b>	2026-04-21 16:20:24 UTC
<b>Description</b>	HTML injection vulnerability in PHP Point of Sale v19.4. This vulnerability allows an attacker to render HTML in the victim's

## Risk And Classification

**Primary CVSS:** v4.0 5.1 MEDIUM from cve-coordination@incibe.es

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:L/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

**EPSS:** 0.000470000 probability, percentile 0.145170000 (date 2026-04-22)

**Problem Types:** CWE-79 | CWE-79 CWE-79 Improper neutralization of input during web page generation ('cross-site scripting')

Version	Source	Type	Score	Severity	Vector
4.0	cve-coordination@incibe.es	Secondary	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:L/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	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:L/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 v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Active

Confidentiality

None

Integrity

None

Availability

None

Sub Conf.

None

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:L/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	<a href="#">PHP Point Of Sale</a>	<a href="#">PHP Point Of Sale</a>	affected 19.4	Not specified

### References

Reference	Source	Link	Tags
<a href="http://www.incibe.es/en/incibe-cert/notices/aviso/html-injection-php-point-sale-0">www.incibe.es/en/incibe-cert/notices/aviso/html-injection-php-point-sale-0</a>	<a href="mailto:cve-coordination@incibe.es">cve-coordination@incibe.es</a>	<a href="http://www.incibe.es">www.incibe.es</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

### Vendor Comments And Credit

#### Discovery Credit

**CNA:** Gonzalo Aguilar García (6h4ack) (en)

### Additional Advisory Data

#### Solutions

**CNA:** There is no solution reported at this time.

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

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)