



# Invoice Ninja Denylist Bypass may Lead to Stored XSS via Invoice Line Items

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

## Summary

<b>CVE</b>	CVE-2026-33628
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-26 21:17:07 UTC
<b>Updated</b>	2026-03-30 17:24:09 UTC

**Description** Invoice Ninja is a source-available invoice, quote, project and time-tracking app built with Laravel. Invoice line item descripti

## Risk And Classification

**Primary CVSS:** v3.1 5.4 MEDIUM from security-advisories@github.com

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

**EPSS:** 0.000390000 probability, percentile 0.117410000 (date 2026-04-01)

**Problem Types:** CWE-79 | CWE-116 | CWE-184 | CWE-79 CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') | CWE-116 CWE-116: Improper Encoding or Escaping of Output | CWE-184 CWE-184: Incomplete List of Disallowed Inputs

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N
3.1	CNA	DECLARED	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

#### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Invoiceninja</a>	<a href="#">Invoice Ninja</a>	All	All	All	All

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Invoiceninja</a>	<a href="#">Invoiceninja</a>	affected < 5.13.4	Not specified

#### References

Reference	Source	Link
<a href="https://github.com/invoiceninja/invoiceninja/security/advisories/GHSA-98wm-cxpw-...">github.com/invoiceninja/invoiceninja/security/advisories/GHSA-98wm-cxpw-...</a>	134c704f-9b21-4f2e-91b3-4a467353bcc0	<a href="#">github.com</a>
<a href="https://github.com/invoiceninja/invoiceninja/releases/tag/v5.13.4">github.com/invoiceninja/invoiceninja/releases/tag/v5.13.4</a>	security-advisories@github.com	<a href="#">github.com</a>
<a href="https://github.com/invoiceninja/invoiceninja/commit/b81a3fc302573fc4a53d61e8537d...">github.com/invoiceninja/invoiceninja/commit/b81a3fc302573fc4a53d61e8537d...</a>	security-advisories@github.com	<a href="#">github.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

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

© 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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)