



# Event Registration Calendar By vcita <= 1.3.1 & Online Payments – Get Paid with PayPal, Square & Stripe <= 3.9.1 - Authenticated (Contributor+) Stored Cross-Site Scripting

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

## Summary

<b>CVE</b>	CVE-2023-2406
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-06-03 05:15:09 UTC
<b>Updated</b>	2026-04-08 17:16:55 UTC
<b>Description</b>	The Event Registration Calendar By vcita plugin, versions up to and including 3.9.1, and Online Payments – Get Paid with f

## Risk And Classification

**Primary CVSS:** v3.1 5.4 MEDIUM from nvd@nist.gov

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

**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
3.1	nvd@nist.gov	Primary	5.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N
3.1	security@wordfence.com	Secondary	6.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N
3.1	CNA	DECLARED	6.4	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/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	Vcita	Event Registration Calendar By Vcita	All	All	All	All
Application	Vcita	Online Payments - Get Paid With Paypal Square Stripe	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Vcita	Event Registration Calendar By Vcita	affected 1.3.1 semver	Not specified
CNA	Vcita	Online Payments Get Paid With PayPal Square Stripe	affected 3.9.1 semver	Not specified

### References

#### Reference

403 Forbidden

Event Registration Calendar By vcita <= 1.3.1 & Online Payments – Get Paid with PayPal, Square & Stripe <= 3.9.1 - Authenticated (Contributor)  
[plugins.trac.wordpress.org/changeset](https://plugins.trac.wordpress.org/changeset)

Security Vulnerabilities in WordPress Plugins by vcita – Jonas' Blog

[plugins.trac.wordpress.org/changeset](https://plugins.trac.wordpress.org/changeset)

[plugins.trac.wordpress.org/changeset/2924423/paypal-payment-button-by-vcita](https://plugins.trac.wordpress.org/changeset/2924423/paypal-payment-button-by-vcita)

403 Forbidden

CVE Program record

NVD vulnerability detail

### Vendor Comments And Credit

Discovery Credit

**CNA:** Jonas Höbenreich (en)

### Additional Advisory Data

Source Time Event

Source	Time	Event
CNA	2023-02-03T00:00:00.000Z	Vendor Notified
CNA	2023-06-02T00:00:00.000Z	Disclosed

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](#).

**Free CVE JSON API** [cve.report/api](#)

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