



# Kali Forms <= 2.1.1 - Cross-Site Request Forgery

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

## Summary

<b>CVE</b>	CVE-2020-36717
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-06-07 02:15:12 UTC
<b>Updated</b>	2026-04-08 19:17:33 UTC
<b>Description</b>	The Kali Forms plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.1.1. Th

## Risk And Classification

**Primary CVSS:** v3.1 8.8 HIGH from nvd@nist.gov

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

**EPSS:** 0.003650000 probability, percentile 0.585130000 (date 2026-04-09)

**Problem Types:** CWE-352 | CWE-352 CWE-352 Cross-Site Request Forgery (CSRF)

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	security@wordfence.com	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

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

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Kaliforms</a>	<a href="#">Kali Forms</a>	All	All	All	All

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Wpchill</a>	<a href="#">Kali Forms Contact Form Drag-and-Drop Builder</a>	affected 2.1.2 semver	Not specified

#### References

Reference	Source	Link
WordPress Kali Forms plugin fixed multiple vulnerabilities. – NinTechNet	af854a3a-2127-422b-91ae-364da2661108	<a href="https://blog.nintech.net">blog.nintech.net</a>
Kali Forms <= 2.1.1 - Cross-Site Request Forgery	af854a3a-2127-422b-91ae-364da2661108	<a href="https://www.wordfence.com">www.wordfence.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

#### Vendor Comments And Credit

Discovery Credit

**CNA:** [Jerome Bruandet \(en\)](#)

#### Additional Advisory Data

Source	Time	Event
CNA	2020-08-21T00:00:00.000Z	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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)