



WordPress Uncanny Toolkit for LearnDash plugin <= 3.6.4.3 - Open Redirection vulnerability

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

Summary

CVE	CVE-2023-34020
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-03-27 14:15:08 UTC
Updated	2026-04-28 19:20:40 UTC
Description	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Uncanny Owl Uncanny Toolkit for LearnDash.This issue

Risk And Classification

Primary CVSS: v3.1 6.1 MEDIUM from nvd@nist.gov

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

Problem Types: CWE-601 | CWE-601 CWE-601 URL Redirection to Untrusted Site ('Open Redirect')

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	audit@patchstack.com	Secondary	4.7	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:N/A:N
3.1	CNA	CVSS	4.7	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:N/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low
 Integrity
 Low
 Availability
 None

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



NVD Known Affected Configurations (CPE 2.3)

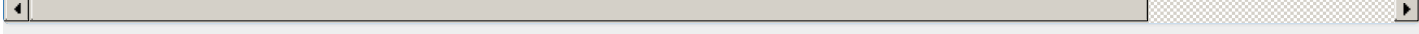
Type	Vendor	Product	Version	Update	Edition	Language
Application	Uncannyowl	Uncanny Toolkit For Learndash	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Uncanny Owl	Uncanny Toolkit For LearnDash	affected n/a 3.6.4.3 custom	Not specified

References

Reference	Source	Link
patchstack.com/database/vulnerability/uncanny-learndash-toolkit/wordpress-un...	af854a3a-2127-422b-91ae-364da2661108	patchstack.c...
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov



Vendor Comments And Credit

Discovery Credit
CNA: Mika (Patchstack Alliance) (en)

Additional Advisory Data

Solutions
CNA: Update to 3.6.4.4 or a higher version.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report