



CVE-2020-11738

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

Summary

CVE	CVE-2020-11738
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-13 22:15:00 UTC
Updated	2022-10-05 16:54:00 UTC
Description	The Snap Creek Duplicator plugin before 1.3.28 for WordPress (and Duplicator Pro before 3.8.7.1) allows Directory Traversal

Risk And Classification

EPSS: 0.942780000 probability, percentile 0.999400000 (date 2026-05-07)

CISA KEV: Listed on 2021-11-03; due 2022-05-03; ransomware use Unknown

Problem Types: CWE-22

CISA Known Exploited Vulnerability

Vendor	WordPress
Product	Snap Creek Duplicator Plugin
Name	WordPress Snap Creek Duplicator Plugin File Download Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2020-11738

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Snapcreek	Duplicator	All	All	All	All
Application	Snapcreek	Duplicator	All	All	All	All
Application	Snapcreek	Duplicator	All	All	All	All
Application	Snapcreek	Duplicator	All	All	All	All
Application	Snapcreek	Duplicator	All	All	All	All

References

Reference	Source	Link	Tags
-----------	--------	------	------

WordPress Duplicator 1.3.26 Arbitrary File Read ≈ Packet Storm	MISC	packetstormsecurity.com	
CWE - CWE-23: Relative Path Traversal (4.3)	MISC	cwe.mitre.org	
Changelog History - Snap Creek Software	MISC	snapcreek.com	Relea
Active Attack on Recently Patched Duplicator Plugin Vulnerability Affects Over 1 Million Sites	MISC	www.wordfence.com	Explo
WordPress Duplicator 1.3.26 Directory Traversal / File Read ≈ Packet Storm	MISC	packetstormsecurity.com	
CVE Program record	CVE.ORG	www.cve.org	canon
NVD vulnerability detail	NVD	nvd.nist.gov	canon
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

730256 WordPress Snap Creek Duplicator and Duplicator Pro Plugins Directory Traversal Vulnerability

© [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