



CVE-2020-28468

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

Summary

CVE	CVE-2020-28468
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-08 12:15:00 UTC
Updated	2021-07-21 11:39:00 UTC
Description	This affects the package pwntools before 4.3.1. The shellcraft generator for affected versions of this module are vulnerable

Risk And Classification

Problem Types: CWE-74

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pwntools Project	Pwntools	All	All	All	All
Application	Pwntools Project	Pwntools	All	All	All	All

References

Reference	Source	Link
Improper Control of Generation of Code ('Code Injection') in pwntools Snyk	MISC	snyk
Fix pwntools shellcraft SSTI vulnerability by Arusekk · Pull Request #1732 · Gallopsled/pwntools · GitHub	MISC	github
Shellcraft generation fails with strings that contains end of multiline comment · Issue #1427 · Gallopsled/pwntools · GitHub	MISC	github
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd

Vendor Comments And Credit

Discovery Credit

LEGACY: Arusekk

Legacy QID Mappings

[981916](#) Python (pip) Security Update for pwntools (GHSA-7xc5-aapp-a249)

© [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](#)