Improper Control of Generation of Code ('Code Injection')

Affecting pwntools package, versions [,4.3.1)

INTRODUCED: 30 NOV 2020 CVE-2020-28468 CWE-94 FIRST ADDED BY SNYK

Share

How to fix?

Upgrade `pwntools` to version 4.3.1 or higher.

Overview

pwntools is a CTF framework and exploit development library. Written in Python, it is designed for rapid prototyping and development, and intended to make exploit writing as simple as possible.

Affected versions of this package are vulnerable to Improper Control of Generation of Code ('Code Injection'). The shellcraft generator for affected versions of this module are vulnerable to Server-Side Template Injection (SSTI), which can lead to remote code execution.

References

- GitHub Issue
- GitHub PR

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	High
Confidentiality	HIGH
Integrity	HIGH
Availability	HIGH

See more

NVD 9.8 CRITICAL

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications

Snyk Learn

Learn about Improper Control of Generation of Code ('Code Injection') vulnerabilities in an interactive lesson.

Start learning

Snyk ID	SNYK-PYTHON-PWNTOOLS-1047345
Published	1 Dec 2020
Disclosed	30 Nov 2020
Credit	Arusekk

Report a new vulnerability | Found a mistake?

RESOURCES

Vulnerability DB

Documentation

Disclosed Vulnerabilities

Blog

FAQs

COMPANY

About

Jobs

Contact

Policies

Do Not Sell My Personal Information

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

Registered in England and Wales. Company number: 09677925

Registered address: Highlands House, Basingstoke Road, Spencers Wood, Reading, Berkshire, RG7 1NT.