

Server-side Request Forgery (SSRF)

Affecting [reportlab](#) package, versions [0,3.5.55)

INTRODUCED: 27 OCT 2020 CVE-2020-28463 CWE-918 FIRST ADDED BY SNYK

Share

How to fix?

Upgrade [reportlab](#) to version 3.5.55 or higher.

Overview

[reportlab](#) is a Python library for generating PDFs and graphics.

Affected versions of this package are vulnerable to Server-side Request Forgery (SSRF) via `img` tags. In order to reduce risk, use `trustedSchemes` & `trustedHosts` (see in [Reportlab's documentation](#)), introduced in version 3.5.55.

Steps to reproduce by Karan Bamal:

1. Download and install the latest package of reportlab
2. Go to demos -> odyssey -> dodyssey
3. In the text file odyssey.txt that needs to be converted to pdf inject ``
4. Create a nc listener `nc -lp 5000`
5. Run `python3 dodyssey.py`
6. You will get a hit on your nc showing we have successfully proceeded to send a server side request
7. `dodyssey.py` will show error since there is no `img` file on the url, but we are able to do SSRF

References

- [Changelog](#)
- [Reportlab Documentation](#)

MEDIUM

Search by package name or CVE

Snyk CVSS

Exploit Maturity Proof of concept

Attack Complexity Low

Confidentiality HIGH

See more

> NVD 6.5 MEDIUM

> Red Hat 6.4 MEDIUM

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 ID SNYK-PYTHON-REPORTLAB-1022145

Published 3 Jan 2021

Disclosed 27 Oct 2020

Credit Karan Bamal

Report a new vulnerability

Found a mistake?

PRODUCT

Snyk Open Source

Snyk Code

Snyk Container

Snyk Infrastructure as Code

Test with Github

Test with CLI

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



© 2022 Snyk Limited

Registered in England and Wales. Company number: 09677925

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