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 `<img src="http://127.0.0.1:5000" valign="top"/>`
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 proceded 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

Snyk CVSS

Exploit Maturity	Proof of concept
Attack Complexity	Low
Confidentiality	HIGH

See more

NVD 6.5 MEDIUM

Red Hat 5.4 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?