



CVE-2020-28463

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

Summary

CVE	CVE-2020-28463
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-18 16:15:00 UTC
Updated	2023-11-07 03:21:00 UTC
Description	All versions of package reportlab are vulnerable to Server-side Request Forgery (SSRF) via img tags. In order to reduce ris

Risk And Classification

Problem Types: CWE-918

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Reportlab	Reportlab	All	All	All	All
Application	Reportlab	Reportlab	All	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 34 Update: python-reportlab-3.6.2-1.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.or
[SECURITY] [DLA 3590-1] python-reportlab security update	MLIST	lists.debian.org
Server-side Request Forgery (SSRF) in reportlab Snyk	CONFIRM	snyk.io
[SECURITY] Fedora 35 Update: python-reportlab-3.6.2-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.or
[SECURITY] Fedora 34 Update: python-reportlab-3.6.2-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.or
[SECURITY] Fedora 35 Update: python-reportlab-3.6.2-1.fc35 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.or
N/A	CONFIRM	www.reportlab.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Karan Bamal

Legacy QID Mappings

[282012](#) Fedora Security Update for python (FEDORA-2021-13cdc0ab0e)

[6000091](#) Debian Security Update for python-reportlab (DLA 3590-1)

[750945](#) OpenSUSE Security Update for python-reportlab (openSUSE-SU-2021:2641-1)

[750958](#) OpenSUSE Security Update for python-reportlab (openSUSE-SU-2021:1147-1)

[980087](#) Python (pip) Security Update for reportlab (GHSA-mpvw-25mg-59vx)

© [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](#)