



CVE-2020-20740

Published on: 11/20/2020 12:00:00 AM UTC

Last Modified on: 01/01/2022 06:10:00 PM UTC

CVE-2020-20740

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

PDFResurrect before 0.20 lack of header validation checks causes heap-buffer-overflow in pdf_get_version().

CVE-2020-20740 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
[SECURITY] Fedora 32 Update: pdfresurrect-0.21-1.fc32 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2020-92195be0e2

[SECURITY] [DLA 2475-1] pdfresurrect security update

lists.debian.org
text/html

MLIST [debian-lts-announce] 20201201 [SECURITY] [DLA 2475-1] pdfresurrect security update

Update header validation checks. · enferex/pdfresurrect@1b42245 · GitHub

Patch
Third Party Advisory
github.com
text/html

MISC
github.com/enferex/pdfresurrect/commit/1b422459f07353adce2878806d5247d9e91f

The lack of a complete magic check leads to heap-buffer-overflow in pdf_get_version() · Issue #14 · enferex/pdfresurrect · GitHub

Exploit
Issue Tracking
Third Party Advisory
github.com
text/html

MISC
github.com/enferex/pdfresurrect/issues/14

[SECURITY] Fedora 33 Update: pdfresurrect-0.21-1.fc33 - package-announce - Fedora Mailing-Lists

lists.fedoraproject.org
text/html

FEDORA FEDORA-2020-e9f9bb77a0

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Pdfresurrect Project	Pdfresurrect	All	All	All	All
Application	Pdfresurrect Project	Pdfresurrect	All	All	All	All
cpe:2.3:o:debian:debian_linux:9.0:*****:						
cpe:2.3:o:fedoraproject:fedora:32:*****:						
cpe:2.3:o:fedoraproject:fedora:33:*****:						
cpe:2.3:a:pdfresurrect_project:pdfresurrect:*****:						
cpe:2.3:a:pdfresurrect_project:pdfresurrect:*****:						

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)

© [CVE.report](#) 2023  |

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)