



CVE-2021-20285

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

Summary

CVE	CVE-2021-20285
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-26 17:15:00 UTC
Updated	2022-08-05 17:44:00 UTC
Description	A flaw was found in upx canPack in p_lx_elf.cpp in UPX 3.96. This flaw allows attackers to cause a denial of service (SEGV

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Upx Project	Upx	3.96	All	All	All

References

Reference	Source	Link
1937787 – (CVE-2021-20285) CVE-2021-20285 upx: Illegal memory access in canPack function in p_lx_elf.cpp	MISC	bug
canPack@p_lx_elf.cpp:2571 BufferOverflow (both latest release version and devel version) · Issue #421 · upx/upx · GitHub	MISC	gith
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvc

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[281483](#) Fedora Security Update for upx (FEDORA-2021-acfb7be76e)

[281484](#) Fedora Security Update for upx (FEDORA-2021-4b43992608)

[281485](#) Fedora Security Update for upx (FEDORA-2021-dff7e97510)

[501701](#) Alpine Linux Security Update for upx

© [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](#)