



CVE-2019-20053

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

Summary

CVE	CVE-2019-20053
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-12-27 22:15:00 UTC
Updated	2022-01-01 20:08:00 UTC
Description	An invalid memory address dereference was discovered in the canUnpack function in p_mach.cpp in UPX 3.95 via a crafted

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Opensuse	Backports	sle-15	sp1	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Application	Upx Project	Upx	3.95	All	All	All
Application	Upx Project	Upx	3.95	All	All	All

References

Reference
[security-announce] openSUSE-SU-2020:0180-1: moderate: Security update f
Segmentation fault (ASAN: SEGV on unknown address) in the PackMachBase<N_Mach::MachClass_64<N_BELE_CTP::LEPolicy> >::canUn
[security-announce] openSUSE-SU-2020:0163-1: moderate: Security update f
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[501262](#) 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](#)