



CVE-2018-11243

Published on: 05/18/2018 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:51:00 AM UTC

CVE-2018-11243

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

Certain versions of [Upx](#) from [Upx Project](#) contain the following vulnerability:

PackLinuxElf64::unpack in p_lx_elf.cpp in UPX 3.95 allows remote attackers to cause a denial of service (double free), limit the ability of a malware scanner to operate on the entire original data, or possibly have unspecified other impact via a crafted file.

CVE-2018-11243 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
Double free (memory clobbered) in PackLinuxElf64::unpack · Issue #207 · upx/upx · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/upx/upx/issues/207

[SECURITY] Fedora 31 Update: upx-3.96-2.fc31 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2020-67590bf08
[security-announce] openSUSE-SU-2020:0180-1: moderate: Security update f	lists.opensuse.org text/html	 SUSE openSUSE-SU-2020:0180
[SECURITY] Fedora 30 Update: upx-3.96-1.fc30 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2020-20cf0743f5
upx/NEWS at devel · upx/upx · GitHub	Release Notes github.com text/html	 MISC github.com/upx/upx/blob/devel/NEWS
[security-announce] openSUSE-SU-2020:0179-1: moderate: Security update f	lists.opensuse.org text/html	 SUSE openSUSE-SU-2020:0179
[security-announce] openSUSE-SU-2020:0162-1: moderate: Security update f	lists.opensuse.org text/html	 SUSE openSUSE-SU-2020:0162
multiple memory reading issue · Issue #206 · upx/upx · GitHub	Exploit Third Party Advisory github.com text/html	 MISC github.com/upx/upx/issues/206
[security-announce] openSUSE-SU-2020:0163-1: moderate: Security update f	lists.opensuse.org text/html	 SUSE openSUSE-SU-2020:0163
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 .		

Related QID Numbers

501262 Alpine Linux Security Update for upx

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Upx Project	Upx	3.95	All	All	All
Application	Upx Project	Upx	3.95	All	All	All
cpe:2.3:a:upx_project:upx:3.95:*:*:*:*:*:						
cpe:2.3:a:upx_project:upx:3.95:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)