



CVE-2020-27788

Published on: Not Yet Published

Last Modified on: 08/22/2022 07:23:00 PM UTC

CVE-2020-27788

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

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

An out-of-bounds read access vulnerability was discovered in UPX in PackLinuxElf64::canPack() function of p_lx_elf.cpp file. An attacker with a crafted input file could trigger this issue that could cause a crash leading to a denial of service.

CVE-2020-27788 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

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

CVE References

Description	Tags	Link
heap-buffer-overflow in PackLinuxElf64::canPack() at p_lx_elf.cpp:2385 · Issue #332 · upx/upx · GitHub	github.com text/html	MISC github.com/upx/upx/issues/332
Detect bad e_shstrtab better. · upx/upx@1bb93d4 · GitHub	github.com text/html	MISC github.com/upx/upx/commit/1bb93d4fce9f1d764ba57bf5ac154af515b3fc83

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
Application	Upx Project	Upx	All	All	All	All
cpe:2.3:a:upx_project:upx:*****:						
No vendor comments have been submitted for this CVE						
Social Mentions						
Source	Title					Posted (UTC)
 @CVereport	CVE-2020-27788 : An out-of-bounds read access vulnerability was discovered in UPX in PackLinuxElf64::canPack func... twitter.com/i/web/status/1...					2022-08-18 20:07:45
← Previous ID			Next ID→			

© [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](#)