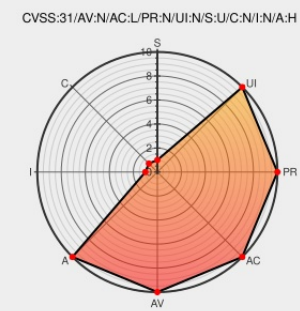
CVE-2021-43312

Published on: Not Yet Published

Last Modified on: 03/28/2023 06:06:00 PM UTC

CVE-2021-43312

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Upx from Upx Project contain the following vulnerability:

A heap-based buffer overflow was discovered in upx, during the variable 'bucket' points to an inaccessible address. The issue is being triggered in the function PackLinuxElf64::invert_pt_dynamic at p_lx_elf.cpp:5239.

CVE-2021-43312 has been assigned by patrick@puiterwijk.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
[bug] heap buffer overflow in PackLinuxElf64::invert_pt_dynamic at p_lx_elf.cpp:5239 · Issue #379 · upx/upx · GitHub	github.com text/html	MISC github.com/upx/upx/issues/379

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-2021-43312 : A heap-based buffer overflow was discovered in upx, during the variable 'bucket' points to an inac… twitter.com/i/web/status/1…	2023-03-24 20:55:13
/r/netcve	CVE-2021-43312	2023-03-24 21:38:44

← Previous ID

Next ID→