



CVE-2019-14295

Published on: 07/27/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:57 PM UTC

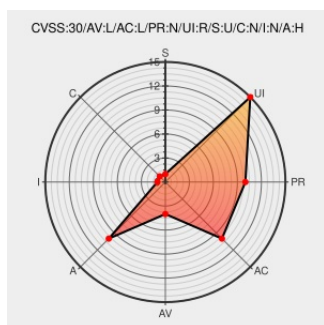
CVE-2019-14295

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

An Integer overflow in the getElfSections function in p_vmlinx.cpp in UPX 3.95 allows remote attackers to cause a denial of service (crash) via a skewed offset larger than the size of the PE section in a UPX packed executable, which triggers an allocation of excessive memory.

CVE-2019-14295 has been assigned by [M](#) cve@mitre.org 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

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Integer-overflow in function getElfSections at p_vmlinx.cpp:119 · Issue #286 · upx/upx · GitHub	Exploit Patch Third Party Advisory github.com text/html	MISC github.com/upx/upx/issues/286

[SECURITY] Fedora 29 Update: upx-3.95-4.fc29 - package-announce - Fedora Mailing-Lists

lists.fedoraproject.org
text/html

 FEDORA FEDORA-2019-
bf4633142b

[SECURITY] Fedora 30 Update: upx-3.95-4.fc30 - package-announce - Fedora Mailing-Lists

lists.fedoraproject.org
text/html

 FEDORA FEDORA-2019-
9a0f02c8c8

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	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→