

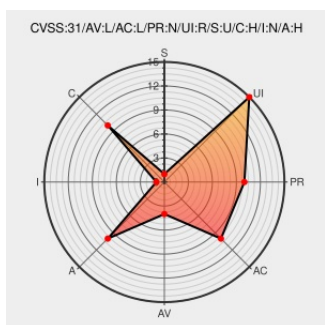


CVE-2020-24119

Published on: 05/14/2021 12:00:00 AM UTC

Last Modified on: 10/26/2022 01:48:00 PM UTC

CVE-2020-24119

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

Certain versions of [Fedora](#) from [Fedoraproject](#) contain the following vulnerability:

A heap buffer overflow read was discovered in upx 4.0.0, because the check in p_lx_elf.cpp is not perfect.

CVE-2020-24119 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.1 - HIGH**

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

CVSS2 Score: **5.8 - MEDIUM**

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

CVE References

Description	Tags	Link
[SECURITY] Fedora 34 Update: upx-3.96-9.fc34 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2021-737766a313
[SECURITY] Fedora 33 Update: upx-3.96-9.fc33 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2021-ceb9db8de0

CWE - CWE-126: Buffer Over-read (4.3)

[cwe.mitre.org](https://cwe.mitre.org/text/html)
text/html

 MISC
cwe.mitre.org/data/definitions/126.html

Heap buffer overflow in get_le32() · Issue #388 · upx/upx · GitHub

github.com
text/html

 CONFIRM
github.com/upx/upx/issues/388

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

[281129](#) Fedora Security Update for upx (FEDORA-2021-ceb9db8de0)

[281130](#) Fedora Security Update for upx (FEDORA-2021-737766a313)

[502959](#) Alpine Linux Security Update for upx

[750184](#) OpenSUSE Security Update for upx (openSUSE-SU-2021:0813-1)

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Application	Upx Project	Upx	4.0.0	All	All	All
cpe:2.3:o:fedoraproject:fedora:33:*****:						
cpe:2.3:o:fedoraproject:fedora:34:*****:						
cpe:2.3:a:upx_project:upx:4.0.0:*****:						

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
 @CVEreport	CVE-2020-24119 : A heap buffer overflow read was discovered in upx 4.0.0, because the check in p_lx_elf.cpp is not... twitter.com/i/web/status/1...	2021-05-14 21:03:20
 /r/netcve	CVE-2020-24119	2021-05-14 21:41:35

[← Previous ID](#)

[Next ID →](#)

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](#)