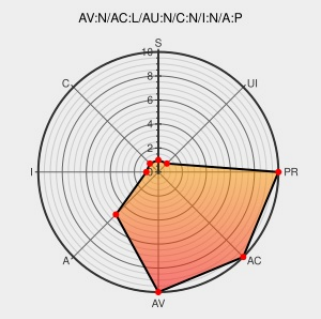
CVE-2014-4715

Published on: 07/02/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:44 PM UTC

CVE-2014-4715

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



Certain versions of Lz4 from Yann Collet contain the following vulnerability:

Yann Collet LZ4 before r119, when used on certain 32-bit platforms that allocate memory beyond 0x80000000, does not properly detect integer overflows, which allows context-dependent attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted Literal Run, a different vulnerability than CVE-2014-4611.

CVE-2014-4715 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
RealTime Data Compression: Vulnerabilities disclosure - how it's supposed to work	web.archive.org, text/html, Inactive Link, Not Archived	CONFIRM fastcompression.blogspot.fr/2014/07/software-vulnerabilities-how-it-works.html
r119 - lz4 - Extremely Fast Compression algorithm - Google Project Hosting	code.google.com, text/html	CONFIRM code.google.com/p/lz4/source/detail?r=119
About Secunia Research | Flexera	secunia.com, Depreciated Link, text/plain	SECUNIA 59770
The Mouse Trap: I Was Wrong - Proving LZ4 Exploitable With Less Than 4MB	blog.securitymouse.com, text/html	MISC blog.securitymouse.com/2014/07/i-was-wrong-proving-lz4-exploitable.html

Issue 134 - lz4 - High Address allocation in 32-bits mode - Extremely Fast Compression algorithm - Google Project Hosting	code.google.com text/html	CONFIRM code.google.com/p/lz4/issues/detail?id=134

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	Yann Collet	Lz4	All	All	All	All

cpe:2.3:a:yann_collet:lz4:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← 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 registred 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