



CVE-2021-29482

Published on: 04/28/2021 12:00:00 AM UTC

Last Modified on: 05/14/2021 07:56:00 PM UTC

CVE-2021-29482 - advisory for GHSA-25xm-hr59-7c27

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

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

xz is a compression and decompression library focusing on the xz format completely written in Go. The function readUvarint used to read the xz container format may not terminate a loop provide malicious input. The problem has been fixed in release v0.5.8. As a workaround users can limit the size of the compressed file input to a reasonable size for their use case. The standard library had recently the same issue and got the CVE-2020-16845 allocated.

CVE-2021-29482 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: ulikunitz - xz version < 0.5.8

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

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
xz: fix a security issue for readUvarint · ulikunitz/xz@69c6093 · GitHub	github.com text/html	 MISC github.com/ulikunitz/xz/commit/69c6093c7b2397b923acf82cb378f55ab2652b9b
Release v0.5.8 fixes readUvarint denial of service · Advisory · ulikunitz/xz · GitHub	github.com text/html	 CONFIRM github.com/ulikunitz/xz/security/advisories/GHSA-25xm-hr59-7c27

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

180034 Debian Security Update for golang-github-ulikunitz-xz (CVE-2021-29482)

982402 Go (go) Security Update for github.com/ulikunitz/xz (GHSA-25xm-hr59-7c27)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xz Project	Xz	All	All	All	All
Application	Xz Project	Xz	All	All	All	All

```
cpe:2.3:a:xz project:xz:*. *. *. *. *. *. *. *. *
```

```
cpe:2.3:a:xz project:xz:*:*:*:*:go:*:*:
```

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-29482 : xz is a compression and decompression library focusing on the xz format completely written in Go.... twitter.com/i/web/status/1...	2021-04-28 18:21:34
 /r/netcve	CVE-2021-29482	2021-04-28 18:42:06

[← 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