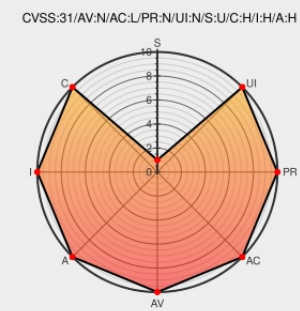
CVE-2014-125026

Published on: Not Yet Published

Last Modified on: 06/12/2023 08:06:25 PM UTC

CVE-2014-125026

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



Certain versions of Golz4 from Cloudflare contain the following vulnerability:

LZ4 bindings use a deprecated C API that is vulnerable to memory corruption, which could lead to arbitrary code execution if called with untrusted user input.

CVE-2014-125026 has been assigned by security@golang.org to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **github.com/cloudflare/golz4** - **github.com/cloudflare/golz4** version **< 0.0.0-20140711154735-199f5f787806**

CVSS3 Score: 9.8 - CRITICAL

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

CVE References

Description	Tags	Link
Use the secure decoder version · Issue #5 · cloudflare/golz4 · GitHub	github.com text/html	MISC github.com/cloudflare/golz4/issues/5
GO-2020-0022 - Go Packages	pkg.go.dev text/html	MISC pkg.go.dev/vuln/GO-2020-0022
Use LZ4_decompress_safe instead of LZ4_uncompress · cloudflare/golz4@199f5f7 · GitHub	github.com text/html	MISC github.com/cloudflare/golz4/commit/199f5f7878062ca17a98e079f2dbe1205e2ed898

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	Cloudflare	Golz4	All	All	All	All

cpe:2.3:a:cloudflare:golz4:*:*:*:*:*:go:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report