



Excessive memory allocation when decoding malicious SFNT in golang.org/x/image

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2026-33812
State	PUBLISHED
Assigner	Go
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-21 20:16:56 UTC
Updated	2026-04-22 21:24:26 UTC
Description	Parsing a malicious font file can cause excessive memory allocation.

Risk And Classification

Primary CVSS: v3.1 6.1 MEDIUM from ADP

CVSS: 3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H

EPSS: 0.000120000 probability, percentile 0.016810000 (date 2026-04-22)

Problem Types: CWE-789: Memory Allocation with Excessive Size Value

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	6.1	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	6.1	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

Low

Integrity

Severity
None

Availability

High

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:H

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Golang.org image	Golang.org/x/image/font/sfnt	affected 0.39.0 semver	Not specified

References

Reference	Source	Link	Tags
pkg.go.dev/vuln/GO-2026-4962	security@golang.org	pkg.go.dev	
go.dev/cl/761180	security@golang.org	go.dev	
go.dev/issue/78382	security@golang.org	go.dev	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Andy Gill, ZephrSec Ltd (en)

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)