



# tinytag: Denial of Service via non-terminating SYLT frame parsing loop

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

## Summary

<b>CVE</b>	CVE-2026-32889
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-20 03:15:59 UTC
<b>Updated</b>	2026-03-30 14:52:35 UTC
<b>Description</b>	tinytag is a Python library for reading audio file metadata. Version 2.2.0 allows an attacker who can supply MP3 files for par

## Risk And Classification

**Primary CVSS:** v3.1 6.5 MEDIUM from security-advisories@github.com

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

**EPSS:** 0.000130000 probability, percentile 0.022210000 (date 2026-04-01)

**Problem Types:** CWE-835 | CWE-835 CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop')

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H
3.1	CNA	DECLARED	6.5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tinytag Project	Tinytag	2.2.0	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Tinytag	Tinytag	affected >= 2.2.0, < 2.2.1	Not specified

### References

Reference	Source	Link	Tags
github.com/tinytag/tinytag/commit/4d649b9c314ada8ff8a74e0469e9aadb3acb252a	security-advisories@github.com	github.com	Patch
github.com/tinytag/tinytag/commit/5cd321521ff097e41724b601d7e3d7adc7e53402	security-advisories@github.com	github.com	Patch
github.com/tinytag/tinytag/security/advisories/GHSA-f4rq-2259-hv29	security-advisories@github.com	github.com	Exploit
github.com/tinytag/tinytag/commit/44e496310f7ced8077e9087e3774acbaa324b18a	security-advisories@github.com	github.com	Patch
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

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.

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)