



CVE-2019-14465

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

Summary

CVE	CVE-2019-14465
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-07-31 23:15:00 UTC
Updated	2023-02-01 20:29:00 UTC
Description	fmt_mtm_load_song in fmt/mtm.c in Schism Tracker 20190722 has a heap-based buffer overflow.

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Schismtracker	Schism Tracker	20190722	All	All	All
Application	Schismtracker	Schism Tracker	20190722	All	All	All

References

Reference	Source	Link
Release Schism Tracker 20190805 · schismtracker/schismtracker · GitHub	MISC	github.co
Schism Tracker: Multiple vulnerabilities (GLSA 202107-12) — Gentoo security	GENTOO	security.
Heap-based buffer overflow in the fmt_mtm_load_song() function · Issue #198 · schismtracker/schismtracker · GitHub	MISC	github.co
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[710064](#) Gentoo Linux Schism Tracker Multiple Vulnerabilities (GLSA 202107-12)

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