



CVE-2021-3403

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2021-3403
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-04 22:15:00 UTC
Updated	2022-04-25 20:17:00 UTC
Description	In ytnef 1.9.3, the TNEFSubjectHandler function in lib/ytnef.c allows remote attackers to cause a denial-of-service (and pote

Risk And Classification

Problem Types: CWE-415

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	FedoraProject	Fedora	33	All	All	All
Operating System	FedoraProject	Fedora	33	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Application	Ytnef Project	Ytnef	1.9.3	All	All	All
Application	Ytnef Project	Ytnef	1.9.3	All	All	All

References

Reference	Source	Li
Double free via TNEFSubjectHandler · Issue #85 · Yeraze/ytnef · GitHub	MISC	gi
1926967 – (CVE-2021-3403) CVE-2021-3403 ytnef: double free in TNEFSubjectHandler function in lib/ytnef.c via crafted file	MISC	bu
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

179881 Debian Security Update for libytnef (CVE-2021-3403)

501725 Alpine Linux Security Update for ytnef

© [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](#)