



# CVE-2020-17448

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2020-17448
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-08-11 17:15:00 UTC
<b>Updated</b>	2021-01-28 18:02:00 UTC
<b>Description</b>	Telegram Desktop through 2.1.13 allows a spoofed file type to bypass the Dangerous File Type Execution protection mech...

## Risk And Classification

**Problem Types:** CWE-863

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Telegram</a>	<a href="#">Telegram Desktop</a>	All	All	All	All

## References

Reference	Source	Link
Release v 2.2.0 · telegramdesktop/tdesktop · GitHub	MISC	<a href="#">github.com</a>
Telegram Desktop: Multiple vulnerabilities (GLSA 202101-34) — Gentoo security	GENTOO	<a href="#">security.gentoo.org</a>
Search web site   Search the web here   Google search   Internet explorer   Search web web   Google	MISC	<a href="#">telegram.org</a>
Vulnerability-Database/Telegram-CVE-2020-17448 at master · VijayT007/Vulnerability-Database · GitHub	MISC	<a href="#">github.com</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

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

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](#)**