



CVE-2021-34858

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2021-34858
State	PUBLIC
Assigner	zdi-disclosures@trendmicro.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-01-13 22:15:00 UTC
Updated	2022-01-21 02:17:00 UTC
Description	This vulnerability allows remote attackers to execute arbitrary code on affected installations of TeamViewer. User interaction

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Teamviewer	Teamviewer	All	All	All	All

References

Reference	Source	Link	Tags
ZDI-21-1001 Zero Day Initiative	MISC	www.zerodayinitiative.com	
August Updates - Security Patches — TeamViewer Support	MISC	community.teamviewer.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[378637](#) TeamViewer File Parsing Out-Of-Bounds Read Remote Code Execution (RCE) Vulnerability

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](#)