



CVE-2020-25507

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

Summary

CVE	CVE-2020-25507
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-28 20:15:00 UTC
Updated	2021-01-04 19:15:00 UTC
Description	An incorrect permission assignment during the installation script of TeamworkCloud 18.0 thru 19.0 allows a local unprivilege

Risk And Classification

Problem Types: CWE-732

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	3ds	Teamwork Cloud	All	All	All	All

References

Reference

- Finding a Vulnerability in Teamwork Cloud Server (NoMagic, 3DS), Which Is Used By Gov/Enterprise to Design Rockets, Missiles, and Satellit Installation on Linux using scripts
- Installation on Linux (RedHat/CentOS 7.x) - Teamwork Cloud 18.5 SP2 - Documentation
- No Magic Community Forum • View topic - Finding and fixing wrong file permission - TWC installation
- Wayback Machine
- security/SICK-2020-002.md at master · sickcodes/security · GitHub
- CVE-2020-25507 - NoMagic (Dassault Systèmes 3DS) Teamwork Cloud 18.0-19.0 - Incorrect Permissions Assignment for a Critical Resource
- CVE Program record
- NVD vulnerability detail

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](#)