



CVE-2023-27830

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

Summary

CVE	CVE-2023-27830
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-04-12 15:15:00 UTC
Updated	2023-04-24 15:59:00 UTC
Description	TightVNC before v2.8.75 allows attackers to escalate privileges on the host operating system via replacing legitimate files v

Risk And Classification

Problem Types: CWE-269

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
TightVNC News	MISC	www.tightvnc.com
Vulnerability Disclosure -Privilege Escalation @ TightVNC by Kartik Lalan NestedIf Mar, 2023 Medium	MISC	medium.com
TightVNC: What's New in TightVNC	MISC	www.tightvnc.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[378487](#) TightVNC Privilege Escalation Vulnerability

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