



CVE-2022-41975

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

Summary

CVE	CVE-2022-41975
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-30 18:15:00 UTC
Updated	2023-08-08 14:22:00 UTC
Description	RealVNC VNC Server before 6.11.0 and VNC Viewer before 6.22.826 on Windows allow local privilege escalation via MSI i

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows	-	All	All	All
Application	Realvnc	Vnc Server	All	All	All	All
Application	Realvnc	Vnc Viewer	All	All	All	All

References

Reference	Source	Link	Tags
Security check	MISC	help.realvnc.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

[378063](#) RealVNC VNC Server and Viewer Local Privilege Escalation Vulnerability (CVE-2022-41975)

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