



CVE-2022-36436

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

Summary

CVE	CVE-2022-36436
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-14 11:15:00 UTC
Updated	2023-08-08 14:22:00 UTC
Description	OSU Open Source Lab VNCAuthProxy through 1.1.1 is affected by an vncap/vnc/protocol.py VNCServerAuthenticator auth

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Osuosl	Twisted Vnc Authentication Proxy	All	All	All	All

References

Reference	Source
VNCAuthProxy · PyPI	MISC
CVE-2022-36436: Twisted VNC Authentication Proxy authentication bypass GRNET CERT	MISC
Fix CVE-2022-36436 - Authentication bypass in RFB security handshake ... · osuosl/twisted_vncauthproxy@edc149a · GitHub	MISC
GitHub - osuosl/twisted_vncauthproxy at release/1.1.1	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report