



Neat VNC: Buffer overflow due to oversized RSA public keys

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

Summary

CVE	CVE-2026-42859
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-11 18:16:36 UTC
Updated	2026-05-11 18:16:36 UTC
Description	Neat VNC is a VNC server library. Prior to 0.9.6, a pre-authentication stack buffer overflow exists in neatvnc in the RSA-AE

Risk And Classification

Primary CVSS: v4.0 8.1 HIGH from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.001290000 probability, percentile 0.317950000 (date 2026-05-12)

Problem Types: CWE-120 | CWE-120 CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	8.1	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	DECLARED	8.1	HIGH	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality	None
Integrity	High
Availability	High
Sub Conf.	None
Sub Integrity	None
Sub Availability	None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Any1	Neatvnc	affected < 0.9.6	Not specified

References

Reference	Source	Link	Tags
github.com/any1/neatvnc/security/advisories/GHSA-567c-gpv8-qh9h	security-advisories@github.com	github.com	
github.com/any1/neatvnc/commit/1f6cd6b75cc167fed3a19a9d1552a1f662f6b337	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.