CVE-2016-9942

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2016-9942
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-12-31 18:59:00 UTC
Updated	2020-10-23 13:15:00 UTC
Description	Heap-based buffer overflow in ultra.c in LibVNCClient in LibVNCServer before 0.9.11 allows remote servers to cause a den

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libvncserver Project	Libvncserver	0.9.10	All	All	All
Application	Libvncserver Project	Libvncserver	0.9.10	All	All	All

References

Reference	Source	Link	Tags
Fix two heap buffer overflows by atalax · Pull Request #137 · LibVNC/libvncserver · GitHub	CONFIRM	github.com	
[SECURITY] [DLA 1979-1] italc security update	MLIST	lists.debian.org	
USN-4587-1: iTALC vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU	usn.ubuntu.com	
Debian -- Security Information -- DSA-3753-1 libvncserver	DEBIAN	www.debian.org	
LibVNCServer Multiple Heap Based Buffer Overflow Vulnerabilities	BID	www.securityfocus.com	
Release LibVNCServer-0.9.11 · LibVNC/libvncserver · GitHub	CONFIRM	github.com	
LibVNCServer/LibVNCClient: Multiple vulnerabilities (GLSA 201702-24) — Gentoo Security	GENTOO	security.gentoo.org	
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

501065 Alpine Linux Security Update for libvncserver

505048 Alpine Linux Security Update for libvncserver

710475 Gentoo Linux LibVNCServer/LibVNCClient Multiple Vulnerabilities (GLSA 201702-24)

Free CVE JSON API cve.report/api

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