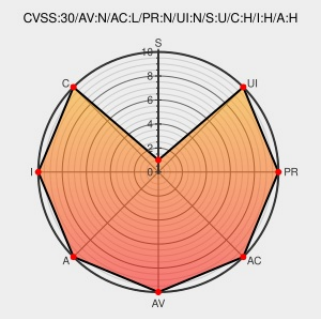
CVE-2016-9941

Published on: 12/31/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:16 PM UTC

CVE-2016-9941

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Libvncserver from Libvncserver Project contain the following vulnerability:

Heap-based buffer overflow in rfbproto.c in LibVNCClient in LibVNCServer before 0.9.11 allows remote servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted FramebufferUpdate message containing a subrectangle outside of the client drawing area.

CVE-2016-9941 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Fix two heap buffer overflows by atalax · Pull Request #137 · LibVNC/libvncserver · GitHub	github.com text/html	CONFIRM github.com/LibVNC/libvncserver/pull/137
[SECURITY] [DLA 1979-1] italc security update	lists.debian.org	MLIST [debian-lts-announce] 20191030 [SECURITY]

[DLA 1979-1] italc security update	text/html	[DLA 1979-1] italc security update
USN-4587-1: iTALC vulnerabilities | Ubuntu security notices | Ubuntu	usn.ubuntu.com text/html	UBUNTU USN-4587-1
Debian -- Security Information -- DSA-3753-1 libvncserver	www.debian.org Depreciated Link text/html	DEBIAN DSA-3753
LibVNCServer Multiple Heap Based Buffer Overflow Vulnerabilities	cve.report (archive) text/html	BID 95170
Release LibVNCServer-0.9.11 · LibVNC/libvncserver · GitHub	github.com text/html	CONFIRM github.com/LibVNC/libvncserver/releases/tag/LibVNCServer-0.9.11
LibVNCServer/LibVNCClient: Multiple vulnerabilities (GLSA 201702-24) — Gentoo Security	security.gentoo.org text/html	GENTOO GLSA-201702-24

Related QID Numbers

501065 Alpine Linux Security Update for libvncserver

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

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:libvncserver_project:libvncserver:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→