

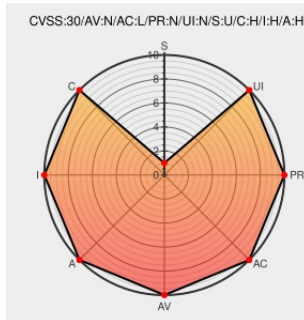


# CVE-2016-9941

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 [M](#) [cve@mitre.org](mailto: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    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **7.5 - HIGH**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>PARTIAL</b>         | <b>PARTIAL</b>    | <b>PARTIAL</b>      |

## CVE References

| Description                                                                                | Tags                                                    | Link                                                            |
|--------------------------------------------------------------------------------------------|---------------------------------------------------------|-----------------------------------------------------------------|
| Fix two heap buffer overflows by atalax · Pull Request #137 · LibVNC/libvncserver · GitHub | <a href="#">github.com</a><br><a href="#">text/html</a> | <a href="#">CONFIRM github.com/LibVNC/libvncserver/pull/137</a> |
| SECURITY ID: A-1979-11 itale security update                                               | <a href="#">lists.debian.org</a>                        | <a href="#">MLIST [debian-lts-announce] 20191030 [SECURITY]</a> |

|                                                                                                        |                                                                                |                                                                                                   |
|--------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| <a href="#">[DEBIAN] [DLA 1979-1] italc security update</a>                                            | <a href="#">lists.debian.org</a><br>text/html                                  | <a href="#">MITRE [Debian] is announced] 20191008 [DEBIAN] [DLA 1979-1] italc security update</a> |
| <a href="#">USN-4587-1: iTALC vulnerabilities   Ubuntu security notices   Ubuntu</a>                   | <a href="#">usn.ubuntu.com</a><br>text/html                                    | <a href="#">UBUNTU USN-4587-1</a>                                                                 |
| <a href="#">Debian -- Security Information -- DSA-3753-1 libvncserver</a>                              | <a href="#">www.debian.org</a><br><a href="#">Deprecated Link</a><br>text/html | <a href="#">DEBIAN DSA-3753</a>                                                                   |
| <a href="#">LibVNCServer Multiple Heap Based Buffer Overflow Vulnerabilities</a>                       | <a href="#">cve.report (archive)</a><br>text/html                              | <a href="#">BID 95170</a>                                                                         |
| <a href="#">Release LibVNCServer-0.9.11 · LibVNC/libvncserver · GitHub</a>                             | <a href="#">github.com</a><br>text/html                                        | <a href="#">CONFIRM github.com/LibVNC/libvncserver/releases/tag/LibVNCServer-0.9.11</a>           |
| <a href="#">LibVNCServer/LibVNCClient: Multiple vulnerabilities (GLSA 201702-24) — Gentoo Security</a> | <a href="#">security.gentoo.org</a><br>text/html                               | <a href="#">GENTOO GLSA-201702-24</a>                                                             |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

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                                        | <a href="#">Libvncserver Project</a> | <a href="#">Libvncserver</a> | All     | All    | All     | All      |
| cpe:2.3:a:libvncserver_project:libvncserver:*****: |                                      |                              |         |        |         |          |

No vendor comments have been submitted for this CVE