



CVE-2018-20750

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2018-20750 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2019-01-30 18:29:00 UTC |
| Updated | 2022-03-09 21:55:00 UTC |
| Description | LibVNC through 0.9.12 contains a heap out-of-bounds write vulnerability in libvncserver/rfbserver.c. The fix for CVE-2018-1 |

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|--------------------------------------|--|---------|--------|---------|----------|
| Operating System | Canonical | Ubuntu Linux | 14.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 16.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 16.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.10 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 14.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 16.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.10 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Application | Libvncserver Project | Libvncserver | All | All | All | All |
| Application | Libvnc Project | Libvncserver | All | All | All | All |
| Hardware | Siemens | Simatic Itc1500 | - | All | All | All |
| Operating System | Siemens | Simatic Itc1500 Firmware | All | All | All | All |
| Hardware | Siemens | Simatic Itc1500 Pro | - | All | All | All |

| | | | | | | |
|------------------|-------------------------|--|-----|-----|-----|-----|
| Operating System | Siemens | Simatic Itc1500 Pro Firmware | All | All | All | All |
| Hardware | Siemens | Simatic Itc1900 | - | All | All | All |
| Operating System | Siemens | Simatic Itc1900 Firmware | All | All | All | All |
| Hardware | Siemens | Simatic Itc1900 Pro | - | All | All | All |
| Operating System | Siemens | Simatic Itc1900 Pro Firmware | All | All | All | All |
| Hardware | Siemens | Simatic Itc2200 | - | All | All | All |
| Operating System | Siemens | Simatic Itc2200 Firmware | All | All | All | All |
| Hardware | Siemens | Simatic Itc2200 Pro | - | All | All | All |
| Operating System | Siemens | Simatic Itc2200 Pro Firmware | All | All | All | All |

References

| Reference | Source | Li |
|--|---------|-----|
| USN-3877-1: LibVNCServer vulnerabilities Ubuntu security notices | UBUNTU | us |
| USN-4547-1: iTALC vulnerabilities Ubuntu security notices Ubuntu | UBUNTU | us |
| oss-security - Re: libvnc and tightvnc vulnerabilities | MISC | w |
| SECURITY: malloc((uint64_t)length + 1) is unsafe, especially on 32-bit systems · Issue #273 · LibVNC/libvncserver · GitHub | MISC | gi |
| LibVNCServer Incomplete Fix Multiple Heap Buffer Overflow Vulnerabilities | BID | w |
| [SECURITY] [DLA 1979-1] italc security update | MLIST | lis |
| [SECURITY] [DLA 1652-1] libvncserver security update | MLIST | lis |
| USN-4587-1: iTALC vulnerabilities Ubuntu security notices Ubuntu | UBUNTU | us |
| Limit length to INT_MAX bytes in rfbProcessFileTransferReadBuffer() · LibVNC/libvncserver@09e8fc0 · GitHub | MISC | gi |
| cert-portal.siemens.com/productcert/pdf/ssa-390195.pdf | CONFIRM | ce |
| CVE Program record | CVE.ORG | w |
| NVD vulnerability detail | NVD | nv |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[590668](#) Siemens SIMATIC ITC Multiple Vulnerabilities (ICSA-21-350-12)

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

