



CVE-2017-2626

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2017-2626 |
| State | PUBLIC |
| Assigner | secalert@redhat.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2018-07-27 19:29:00 UTC |
| Updated | 2023-02-12 23:29:00 UTC |
| Description | It was discovered that libICE before 1.0.9-8 used a weak entropy to generate keys. A local attacker could potentially use thi |

Risk And Classification

Problem Types: CWE-331

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|-----------------------------|--|---------|--------|---------|----------|
| Application | Freedesktop | Libice | All | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus | 7.4 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus | 7.4 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.4 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.5 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.4 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.5 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 7.0 | All | All | All |

References

| Reference | Source | Link |
|--|--------|--------------------|
| Bug 1424992 – CVE-2017-2626 libICE: weak entropy usage in session keys | MISC | bu |

| | | |
|--|----------|----------------------|
| Red Hat Customer Portal | REDHAT | ac |
| 1424992 – (CVE-2017-2626) CVE-2017-2626 libICE: weak entropy usage in session keys | CONFIRM | bu |
| [SECURITY] [DLA 2002-1] libice security update | MLIST | list |
| X.org X Server Local Multiple Security Vulnerabilities | BID | ww |
| X Multiple Flaws Let Local Users Conduct Timing and Key Guessing Attacks Obtain Elevated Privileges - SecurityTracker | SECTRACK | ww |
| xorg/lib/libICE - Inter-Client Exchange library (mirrored from https://gitlab.freedesktop.org/xorg/lib/libice) | CONFIRM | cgi |
| Advisory X41-2017-001: Multiple Vulnerabilities in X.org - X41 D-SEC GmbH | MISC | ww |
| CVE-2017-2626 - Red Hat Customer Portal | MISC | ac |
| X.Org: Multiple vulnerabilities (GLSA 201704-03) — Gentoo Security | GENTOO | se |
| oss-security - Fwd: [ANNOUNCE] libICE 1.0.10 | MLIST | ww |
| CVE Program record | CVE.ORG | ww |
| NVD vulnerability detail | NVD | nvd |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[199048](#) Ubuntu Security Notification for libICE Vulnerability (USN-5744-1)

[500297](#) Alpine Linux Security Update for libice

[504062](#) Alpine Linux Security Update for libice

[710339](#) Gentoo Linux X.Org Multiple Vulnerabilities (GLSA 201704-03)

© [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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)