



CVE-2016-5824

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

Summary

CVE	CVE-2016-5824
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-27 22:59:00 UTC
Updated	2019-04-02 07:29:00 UTC
Description	libical 1.0 allows remote attackers to cause a denial of service (use-after-free) via a crafted ics file.

Risk And Classification

Problem Types: CWE-416

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	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
Application	Libical Project	Libical	1.0	All	All	All
Application	Libical Project	Libical	1.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All

Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All

References

Reference	Source	Link
USN-3897-1: Thunderbird vulnerabilities Ubuntu security notices	UBUNTU	usn.ubuntu.com
libical Multiple Heap Overflow Vulnerabilities	BID	www.securityfocus.com
CVE-2016-5824: use-after-free issues · Issue #286 · libical/libical · GitHub	CONFIRM	github.com
Libical: Multiple vulnerabilities (GLSA 201904-02) — Gentoo security	GENTOO	security.gentoo.org
Potentially security-sensitive crashes, best way to get them to you? · Issue #235 · libical/libical · GitHub	MISC	github.com
oss-security - Re: libical 0.47 SEGV on unknown address	MLIST	www.openwall.com
Red Hat Customer Portal	REDHAT	access.redhat.com
oss-security - Re: CVE-2016-9584: heap use-after-free on libical	MLIST	www.openwall.com
1275400 – (CVE-2016-5824) Handful use-after-free crashes in libical (used in Thunderbird)	CONFIRM	bugzilla.mozilla.org
Mozilla Thunderbird and Firefox: Multiple vulnerabilities (GLSA 201904-07) — Gentoo Security	GENTOO	security.gentoo.org
A heap-buffer-overflow in icaltime_from_string · Issue #251 · libical/libical · GitHub	CONFIRM	github.com
Red Hat Customer Portal	REDHAT	access.redhat.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[710177](#) Gentoo Linux Mozilla Thunderbird and Firefox Multiple vulnerabilities (GLSA 201904-07)

[710182](#) Gentoo Linux Libical Multiple vulnerabilities (GLSA 201904-02)

© [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](#)