



CVE-2015-0247

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

Summary

CVE	CVE-2015-0247
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-02-17 15:59:00 UTC
Updated	2018-10-09 19:55:00 UTC
Description	Heap-based buffer overflow in opensfs.c in the libext2fs library in e2fsprogs before 1.42.12 allows local users to execute arbitrary code with root privileges.

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Application	E2fsprogs Project	E2fsprogs	All	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All
Operating System	Fedoraproject	Fedora	20	All	All	All
Operating System	Fedoraproject	Fedora	21	All	All	All

References

Reference

1187032 – (CVE-2015-0247) CVE-2015-0247 e2fsprogs: ext2fs_open2() missing first_meta_bg boundary check leading to heap buffer overflow

[SECURITY] Fedora 21 Update: e2fsprogs-1.42.12-3.fc21

Debian -- Security Information -- DSA-3166-1 e2fsprogs

Support / Security / Advisories // MDVSA-2015:067 | Mandriva

SecurityFocus

e2fsprogs: Heap-based buffer overflow (GLSA 201701-06) — Gentoo security

[SECURITY] Fedora 21 Update: e2fsprogs-1.42.12-1.fc21

Mageia Advisory: MGASA-2015-0061 - Updated e2fsprogs packages fix CVE-2015-0247

[SECURITY] Fedora 20 Update: e2fsprogs-1.42.12-3.fc20

ext2/e2fsprogs.git - Ext2/3/4 filesystem userspace utilities

e2fsprogs 'lib/ext2fs/openfs.c' Local Heap Based Buffer Overflow Vulnerability

USN-2507-1: e2fsprogs vulnerabilities | Ubuntu

e2fsprogs Input Sanitization ≈ Packet Storm

[security-announce] SUSE-SU-2015:1103-1: important: Security update for

Support / Security / Advisories // MDVSA-2015:045 | Mandriva

IBM X-Force Exchange

openSUSE-SU-2015:1006-1: moderate: Security update for e2fsprogs

oCERT.org - oCERT Advisories

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[710444](#) Gentoo Linux e2fsprogs Heap-based buffer overflow Vulnerability (GLSA 201701-06)

© [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](#)