



CVE-2015-1862

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

Summary

CVE	CVE-2015-1862
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-02-09 22:29:00 UTC
Updated	2018-03-08 16:03:00 UTC
Description	The crash reporting feature in Abrt allows local users to gain privileges by leveraging an execve by root after a chroot into a

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Abrt Project	Abrt	All	All	All	All

References

Reference	Source	Link
oss-security - Problems in automatic crash analysis frameworks	MLIST	www.openwall.com
Fedora abrt Race Condition ≈ Packet Storm	MISC	packetstormsecurity.com
Abrt (Fedora 21) - Race Condition - Linux local Exploit	EXPLOIT-DB	www.exploit-db.com
1211223 – (CVE-2015-1862) CVE-2015-1862 abrt: local privilege escalation through kernel.core_pattern	CONFIRM	bugzilla.redhat.com
Abrt / Apport Race Condition / Symlink ≈ Packet Storm	MISC	packetstormsecurity.com
Support handling crashes in lxc containers by sorki · Pull Request #810 · abrt/abrt · GitHub	CONFIRM	github.com
Apport/Abrt (Ubuntu / Fedora) - Local Privilege Escalation - Linux local Exploit	EXPLOIT-DB	www.exploit-db.com
Abrt CVE-2015-1862 Local Privilege Escalation Vulnerability	BID	www.securityfocus.com
Full Disclosure: Problems in automatic crash analysis frameworks	FULLDISC	seclists.org
Linux Apport/Abrt Local Root Exploit ≈ Packet Storm	MISC	packetstormsecurity.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.

There are currently no legacy QID mappings associated with this CVE.

© [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](#).

Free CVE JSON API [cve.report/api](#)

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