



CVE-2015-5231

Published on: 06/07/2016 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:08:11 AM UTC

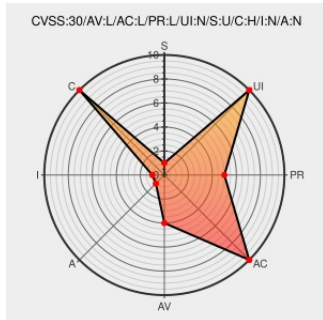
CVE-2015-5231

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Checkpoint/restore In Userspace](#) from [Criu](#) contain the following vulnerability:

The service daemon in CRIU does not properly restrict access to non-dumpable processes, which allows local users to obtain sensitive information via (1) process dumps or (2) ptrace access.

CVE-2015-5231 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: **2.1 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
[CRIU] Hardening the criu service daemon	Vendor Advisory lists.openvz.org text/html	MLIST [CRIU] 20150825 Hardening the criu service daemon
openSUSE-SU-2015:1593-1: moderate: Security update for	lists.opensuse.org	SUSE openSUSE-SU-2015:1593

criu

text/html

oss-security - CVE-2015-5228 & CVE-2015-5231 in the criu service daemon

[www.openwall.com](#)
text/html

 [MLIST \[oss-security\] 20150825 CVE-2015-5228 & CVE-2015-5231 in the criu service daemon](#)

1256728 – (CVE-2015-5231) CVE-2015-5231 criu: service daemon allows to bypass ptrace policy

[bugzilla.redhat.com](#)
text/html

 [CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1256728](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Criu	Checkpoint/restore In Userspace	-	All	All	All
Application	Criu	Checkpoint/restore In Userspace	-	All	All	All
Application	Criu	Checkpoint/restore In Userspace	-	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All

cpe:2.3:a:criu:checkpoint/restore_in_userspace:-:*:*:*:*:*:

cpe:2.3:a:criu:checkpoint\restore_in_userspace:-:*:*:*:*:*:

cpe:2.3:a:criu:checkpoint\restore_in_userspace:-:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:13.2:*:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:13.2:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →