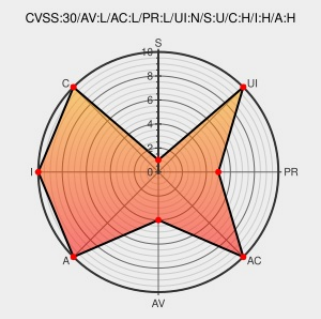
CVE-2015-5228

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

Last Modified on: 02/12/2023 11:12:04 PM UTC

CVE-2015-5228

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 creates log and dump files insecurely, which allows local users to create arbitrary files and take ownership of existing files via unspecified vectors related to a directory path.

CVE-2015-5228 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

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	lists.opensuse.org	SUSE openSUSE-SU-2015:1593

update for criu	text/html	
Bug 1255782 – CVE-2015-5228 criu: arbitrary file creation and chown	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1255782
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

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→