



CVE-2014-8171

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

Summary

CVE	CVE-2014-8171
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-02-09 22:29:00 UTC
Updated	2023-02-13 00:44:00 UTC
Description	The memory resource controller (aka memcg) in the Linux kernel allows local users to cause a denial of service (deadlock)

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Application	Redhat	Enterprise Mrg	2.0	All	All	All
Operating System	Redhat	Enterprise Mrg	2.0	All	All	All
Application	Redhat	Enterprise Mrg	2.0	All	All	All

References

Reference	Source	Link	Tags
Linux Kernel CVE-2014-8171 Denial of Service Vulnerability	BID	www.securityfocus.com	Third Party Advis
1198109 – (CVE-2014-8171) CVE-2014-8171 kernel: memcg: OOM handling DoS	CONFIRM	bugzilla.redhat.com	Issue Tracking, T
Red Hat Customer Portal	MISC	access.redhat.com	
Red Hat Customer Portal	MISC	access.redhat.com	
Red Hat Customer Portal	REDHAT	rhn.redhat.com	Third Party Advis

Red Hat Customer Portal	REDHAT	rhn.redhat.com	Third Party Adviser
Red Hat Customer Portal	REDHAT	rhn.redhat.com	Third Party Adviser
Red Hat Customer Portal	MISC	access.redhat.com	
Red Hat Customer Portal	MISC	access.redhat.com	
access.redhat.com CVE-2014-8171	MISC	access.redhat.com	
Red Hat Customer Portal	REDHAT	rhn.redhat.com	Third Party Adviser
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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