



CVE-2014-3940

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

Summary

CVE	CVE-2014-3940
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-06-05 17:55:00 UTC
Updated	2021-07-15 19:16:00 UTC
Description	The Linux kernel through 3.14.5 does not properly consider the presence of hugetlb entries, which allows local users to cau

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	3.14	-	All	All
Operating System	Linux	Linux Kernel	3.14	rc1	All	All
Operating System	Linux	Linux Kernel	3.14	rc2	All	All
Operating System	Linux	Linux Kernel	3.14	rc3	All	All
Operating System	Linux	Linux Kernel	3.14	rc4	All	All
Operating System	Linux	Linux Kernel	3.14	rc5	All	All
Operating System	Linux	Linux Kernel	3.14	rc6	All	All
Operating System	Linux	Linux Kernel	3.14	rc7	All	All
Operating System	Linux	Linux Kernel	3.14	rc8	All	All
Operating System	Linux	Linux Kernel	3.14.1	All	All	All
Operating System	Linux	Linux Kernel	3.14.2	All	All	All
Operating System	Linux	Linux Kernel	3.14.3	All	All	All
Operating System	Linux	Linux Kernel	3.14.4	All	All	All
Operating System	Linux	Linux Kernel	3.14	-	All	All
Operating System	Linux	Linux Kernel	3.14	rc1	All	All
Operating System	Linux	Linux Kernel	3.14	rc2	All	All
Operating System	Linux	Linux Kernel	3.14	rc3	All	All

Operating System	Linux	Linux Kernel	3.14	rc4	All	All
Operating System	Linux	Linux Kernel	3.14	rc5	All	All
Operating System	Linux	Linux Kernel	3.14	rc6	All	All
Operating System	Linux	Linux Kernel	3.14	rc7	All	All
Operating System	Linux	Linux Kernel	3.14	rc8	All	All
Operating System	Linux	Linux Kernel	3.14.1	All	All	All
Operating System	Linux	Linux Kernel	3.14.2	All	All	All
Operating System	Linux	Linux Kernel	3.14.3	All	All	All
Operating System	Linux	Linux Kernel	3.14.4	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	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	
Red Hat Customer Portal				REDHAT	rhn.rec	
Security Advisory SA59011 - Linux Kernel HugeTBL Entries Denial of Service Vulnerability - Secunia				SECUNIA	secuni	
Bug 1104097 – CVE-2014-3940 Kernel: missing check during hugepage migration				CONFIRM	bugzilla	
Security Advisory SA61310 - F5 Multiple Products Linux Kernel Two Vulnerabilities - Secunia				SECUNIA	secuni	
SOL15685 - Linux kernel vulnerability CVE-2014-3940				CONFIRM	suppor	
oss-security - CVE-2014-3940 - Linux kernel - missing check during hugepage migration				MLIST	www.o	
Linux Kernel CVE-2014-3940 Unspecified Security Vulnerability				BID	www.s	
LKML: Naoya Horiguchi: [PATCH RESEND -mm 1/2] mm: add lpte_present() check on existing hugetlb_entry callbacks				MLIST	lkml.or	
Red Hat Customer Portal				REDHAT	rhn.rec	
CVE Program record				CVE.ORG	www.c	
NVD vulnerability detail				NVD	nvd.nis	

No vendor comments have been submitted for this CVE.

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

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