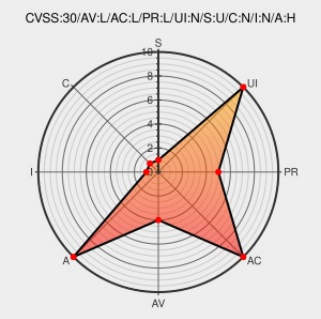
CVE-2017-15128

Published on: 01/14/2018 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:12:05 PM UTC

CVE-2017-15128

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Linux Kernel from Linux contain the following vulnerability:

A flaw was found in the hugetlb_mcopy_atomic_pte function in mm/hugetlb.c in the Linux kernel before 4.13.12. A lack of size check could cause a denial of service (BUG).

CVE-2017-15128 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	NONE	NONE	HIGH

CVSS2 Score: 4.9 - MEDIUM

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

CVE References

Description	Tags	Link
	Issue Tracking Release Notes Vendor Advisory www.kernel.org text/plain	MISC www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.13.12

userfaultfd: hugetlbfs: prevent UFFDIO_COPY to fill beyond the end of… · torvalds/linux@1e39214 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/torvalds/linux/commit/1e3921471354244f70fe268586ff94a97a6dd4df
kernel/git/torvalds/linux.git - Linux kernel source tree	Patch Vendor Advisory git.kernel.org text/html	MISC git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=1e3921471354244f70fe268586ff94a97a6dd4df
CVE-2017-15128 - Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	MISC access.redhat.com/security/cve/CVE-2017-15128
1525222 – (CVE-2017-15128) CVE-2017-15128 kernel: Out of bound access in hugetlb_mcopy_atomic_pte function in mm/hugetlb.c	Issue Tracking Patch Third Party Advisory bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1525222

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	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

cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:enterprise_mrg:2.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_mrg:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:enterprise_mrg:2.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report