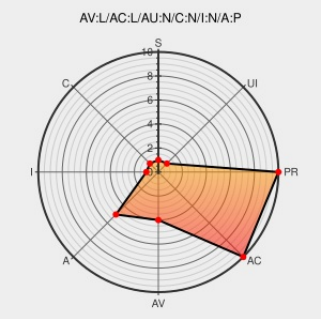
CVE-2005-2100

Published on: 10/25/2005 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:09:26 AM UTC

CVE-2005-2100

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



Certain versions of Enterprise Linux from Redhat contain the following vulnerability:

The rw_vm function in usercopy.c in the 4GB split patch for the Linux kernel in Red Hat Enterprise Linux 4 does not perform proper bounds checking, which allows local users to cause a denial of service (crash).

CVE-2005-2100 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 2.1 - LOW

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

CVE References

Description	Tags	Link
rhn.redhat.com | Red Hat Support	Vendor Advisory, www.redhat.com, text/html	REDHAT RHSA-2005:514
Secunia - Advisories - Red Hat update for kernel	web.archive.org, text/html	SECUNIA 17073
165547 – CAN-2005-2100 4G/4G split bounds checking	Patch, bugzilla.redhat.com, text/html	CONFIRM bugzilla.redhat.com/bugzilla/show_bug.cgi?id=165547
Repository / Oval Repository	oval.cisecurity.org, text/html	OVAL oval:org.mitre.oval:def:11556

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
Operating System	Redhat	Enterprise Linux	4.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	workstation	All
Operating System	Redhat	Enterprise Linux	4.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	4.0	All	workstation	All
Operating System	Redhat	Enterprise Linux Desktop	4.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	4.0	All	All	All

cpe:2.3:o:redhat:enterprise_linux:4.0:*:advanced_server:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:4.0:*:enterprise_server:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:4.0:*:workstation:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:4.0:*:advanced_server:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:4.0:*:enterprise_server:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux:4.0:*:workstation:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_desktop:4.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_desktop:4.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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