



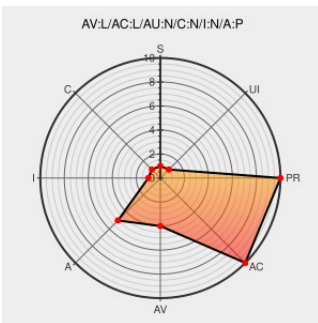
Last Modified on: 03/23/2021 11:27:27 PM UTC

CVE-2005-0090

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of [Enterprise Linux](#) from [Redhat](#) contain the following vulnerability:

A regression error in the Red Hat Enterprise Linux 4 kernel 4GB/4GB split patch omits an "access check," which allows local users to cause a denial of service (crash).

CVE-2005-0090 has been assigned by cve@mitre.org 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
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF red-hat-regression-dos(20618)
rhn.redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2005:092
Red Hat Enterprise Linux Kernel Multiple Vulnerabilities	Vendor Advisory cve.report (archive) text/html	 BID 12599
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval.org.mitre.oval:def:10425

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 info@CVE.org.

This report does not endorse any commercial products that may be mentioned in these entries. 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 →](#)

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)