

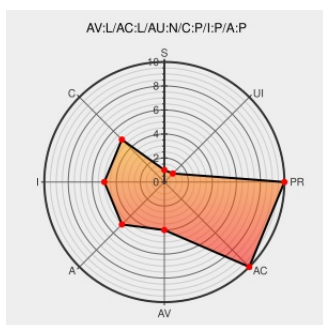


CVE-2005-3631

Published on: 12/22/2005 12:00:00 AM UTC

Last Modified on: 02/13/2023 02:10:42 AM UTC

CVE-2005-3631

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

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

udev does not properly set permissions on certain files in `/dev/input`, which allows local users to obtain sensitive data that is entered at the console, such as user passwords.

CVE-2005-3631 has been assigned by [secalert@redhat.com](#) to track the vulnerability

CVSS2 Score: **4.6 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

SecurityTracker.com Archives - udev Insecure File Permissions in '/dev/input' May Let Local Users Obtain Sensitive Information

[securitytracker.com](#)
text/html

[SECTrack 1015386](#)

RedHat Enterprise Linux UDEV Insecure Permissions Vulnerability

[Patch](#)
[cve.report \(archive\)](#)
text/html

[BID 15994](#)

Secunia - Advisories - Red Hat update for udev

[Patch](#)
[Vendor Advisory](#)
[web.archive.org](#)
text/html

[SECUNIA 18193](#)

Repository / Oval Repository

[oval.cisecurity.org](#)
text/html

[OVAL](#)
oval.org.mitre.oval:def:10854

[rhnl.redhat.com](#) | Red Hat Support

[Patch](#)
[Vendor Advisory](#)

[REDHAT RHSA-2005:864](#)

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 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

© [CVE.report](#) 2023  |

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](#).

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