

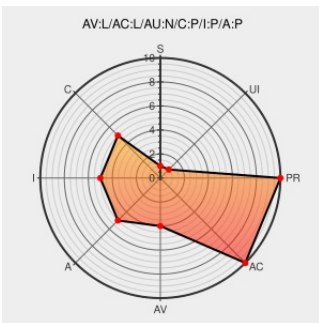


CVE-2005-1194

Published on: 05/04/2005 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:09:25 AM UTC

CVE-2005-1194

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

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

Stack-based buffer overflow in the `ieee_putascii` function for `nasm` 0.98 and earlier allows attackers to execute arbitrary code via a crafted asm file, a different vulnerability than CVE-2004-1287.

CVE-2005-1194 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

rhn.redhat.com | Red Hat Support

[Patch](#)
[Vendor Advisory](#)
www.redhat.com
[text/html](#)

[REDHAT RHSA-2005:381](#)

Repository / Oval Repository

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

[OVAL oval:org.mitre.oval:def:11256](#)

NASM IEEE_PUTASCII Remote Buffer Overflow Vulnerability

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

[BID 13506](#)

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	2.1	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	2.1	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	2.1	All	workstation	All
Operating System	Redhat	Enterprise Linux	3.0	All	advanced_servers	All
Operating System	Redhat	Enterprise Linux	3.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	3.0	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	2.1	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	2.1	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	2.1	All	workstation	All
Operating System	Redhat	Enterprise Linux	3.0	All	advanced_servers	All
Operating System	Redhat	Enterprise Linux	3.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	3.0	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	3.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	4.0	All	All	All

Operating System	Redhat	Enterprise Linux Desktop	3.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	4.0	All	All	All
Operating System	Redhat	Linux Advanced Workstation	2.1	All	ia64	All
Operating System	Redhat	Linux Advanced Workstation	2.1	All	ia64	All
cpe:2.3:o:redhat:enterprise_linux:2.1*:advanced_server:*****:						
cpe:2.3:o:redhat:enterprise_linux:2.1*:enterprise_server:*****:						
cpe:2.3:o:redhat:enterprise_linux:2.1*:workstation:*****:						
cpe:2.3:o:redhat:enterprise_linux:3.0*:advanced_servers:*****:						
cpe:2.3:o:redhat:enterprise_linux:3.0*:enterprise_server:*****:						
cpe:2.3:o:redhat:enterprise_linux:3.0*: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:2.1*:advanced_server:*****:						
cpe:2.3:o:redhat:enterprise_linux:2.1*:enterprise_server:*****:						
cpe:2.3:o:redhat:enterprise_linux:2.1*:workstation:*****:						
cpe:2.3:o:redhat:enterprise_linux:3.0*:advanced_servers:*****:						
cpe:2.3:o:redhat:enterprise_linux:3.0*:enterprise_server:*****:						
cpe:2.3:o:redhat:enterprise_linux:3.0*: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:3.0*:*****:						
cpe:2.3:o:redhat:enterprise_linux_desktop:4.0*:*****:						
cpe:2.3:o:redhat:enterprise_linux_desktop:3.0*:*****:						
cpe:2.3:o:redhat:enterprise_linux_desktop:4.0*:*****:						
cpe:2.3:o:redhat:linux_advanced_workstation:2.1*:ia64:*****:						

cpe:2.3:o:redhat:linux_advanced_workstation:2.1:::lab4:0:0:0:0

← Previous ID

Next ID→

© [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](#)