



CVE-2004-0138

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:11 PM UTC

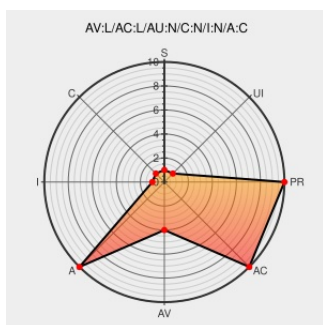
CVE-2004-0138

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

The ELF loader in Linux kernel 2.4 before 2.4.25 allows local users to cause a denial of service (crash) via a crafted ELF file with an interpreter with an invalid arch (architecture), which triggers a BUG() when an invalid VMA is unmapped.

CVE-2004-0138 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.9 - MEDIUM**

Access Vector

LOCAL

Access Complexity

LOW

Authentication

NONE

Confidentiality Impact

NONE

Integrity Impact

NONE

Availability Impact

COMPLETE

CVE References

Description

Tags

Link

Debian -- Security Information -- DSA-1067-1
kernel-source-2.4.16

[Patch](#)
[Vendor Advisory](#)
[www.debian.org](#)
[Deprecated Link](#)
[text/html](#)

[DEBIAN DSA-1067](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF linux-kernel-elfloader-dos\(43124\)](#)

rhn.redhat.com | Red Hat Support

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

[REDHAT RHSA-2004:504](#)

Debian -- Security Information -- DSA-1070-1
kernel-source-2.4.19

[Patch](#)
[Vendor Advisory](#)
[www.debian.org](#)
[Deprecated Link](#)
[text/html](#)

[DEBIAN DSA-1070](#)

Debian -- Security Information -- DSA-1082-1 kernel-source-2.4.17	Patch Vendor Advisory www.debian.org Deprecated Link text/html	 DEBIAN DSA-1082
	kernel.org text/plain	 CONFIRM kernel.org/pub/linux/kernel/v2.4/ChangeLog-2.4.25
Secunia - Advisories - Debian update for kernel-source-2.4.16	Patch Vendor Advisory web.archive.org text/html	 SECUNIA 20162
redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2004:549
Linux Kernel ELF Loader Mismatched Architecture Local Denial of Service Vulnerability	cve.report (archive) text/html	 BID 18174
Secunia - Advisories - Debian update for kernel-source-2.4.18	Patch Vendor Advisory web.archive.org text/html	 SECUNIA 20202
Secunia - Advisories - Debian update for kernel-source-2.4.17	web.archive.org text/html	 SECUNIA 20338
No Description Provided	kernel.debian.net Inactive Link Not Archived	 CONFIRM kernel.debian.net/debian/pool/main/kernel-source-2.4.17/kernel-source-2.4.17_2.4.17-1woody4_ia64.changes
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:10123
No Description Provided	linux.bkbits.net Inactive Link Not Archived	 CONFIRM linux.bkbits.net:8080/linux-2.4/cset@4021346f79nBb-4X_usRikR3Iyb4Vg
Debian -- Security Information -- DSA-1069-1 kernel-source-2.4.18	Patch Vendor Advisory www.debian.org Deprecated Link text/html	 DEBIAN DSA-1069
Secunia - Advisories - Debian update for kernel-source-2.4.19	Patch Vendor Advisory web.archive.org text/html	 SECUNIA 20163

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	Linux	Linux Kernel	2.4.0	All	All	All

System						
Operating System	Linux	Linux Kernel	2.4.1	All	All	All
Operating System	Linux	Linux Kernel	2.4.10	All	All	All
Operating System	Linux	Linux Kernel	2.4.11	All	All	All
Operating System	Linux	Linux Kernel	2.4.12	All	All	All
Operating System	Linux	Linux Kernel	2.4.13	All	All	All
Operating System	Linux	Linux Kernel	2.4.14	All	All	All
Operating System	Linux	Linux Kernel	2.4.15	All	All	All
Operating System	Linux	Linux Kernel	2.4.16	All	All	All
Operating System	Linux	Linux Kernel	2.4.17	All	All	All
Operating System	Linux	Linux Kernel	2.4.18	All	All	All
Operating System	Linux	Linux Kernel	2.4.19	All	All	All
Operating System	Linux	Linux Kernel	2.4.2	All	All	All
Operating System	Linux	Linux Kernel	2.4.20	All	All	All
Operating System	Linux	Linux Kernel	2.4.21	All	All	All
Operating System	Linux	Linux Kernel	2.4.22	All	All	All
Operating System	Linux	Linux Kernel	2.4.23	All	All	All
Operating System	Linux	Linux Kernel	2.4.24	All	All	All
Operating System	Linux	Linux Kernel	2.4.3	All	All	All
Operating System	Linux	Linux Kernel	2.4.4	All	All	All
Operating System	Linux	Linux Kernel	2.4.5	All	All	All
Operating System	Linux	Linux Kernel	2.4.6	All	All	All
Operating System	Linux	Linux Kernel	2.4.7	All	All	All
Operating System	Linux	Linux Kernel	2.4.8	All	All	All

System						
Operating System	Linux	Linux Kernel	2.4.9	All	All	All
Operating System	Linux	Linux Kernel	2.4.0	All	All	All
Operating System	Linux	Linux Kernel	2.4.1	All	All	All
Operating System	Linux	Linux Kernel	2.4.10	All	All	All
Operating System	Linux	Linux Kernel	2.4.11	All	All	All
Operating System	Linux	Linux Kernel	2.4.12	All	All	All
Operating System	Linux	Linux Kernel	2.4.13	All	All	All
Operating System	Linux	Linux Kernel	2.4.14	All	All	All
Operating System	Linux	Linux Kernel	2.4.15	All	All	All
Operating System	Linux	Linux Kernel	2.4.16	All	All	All
Operating System	Linux	Linux Kernel	2.4.17	All	All	All
Operating System	Linux	Linux Kernel	2.4.18	All	All	All
Operating System	Linux	Linux Kernel	2.4.19	All	All	All
Operating System	Linux	Linux Kernel	2.4.2	All	All	All
Operating System	Linux	Linux Kernel	2.4.20	All	All	All
Operating System	Linux	Linux Kernel	2.4.21	All	All	All
Operating System	Linux	Linux Kernel	2.4.22	All	All	All
Operating System	Linux	Linux Kernel	2.4.23	All	All	All
Operating System	Linux	Linux Kernel	2.4.24	All	All	All
Operating System	Linux	Linux Kernel	2.4.3	All	All	All
Operating System	Linux	Linux Kernel	2.4.4	All	All	All
Operating System	Linux	Linux Kernel	2.4.5	All	All	All
Operating System	Linux	Linux Kernel	2.4.6	All	All	All

System						
Operating System	Linux	Linux Kernel	2.4.7	All	All	All
Operating System	Linux	Linux Kernel	2.4.8	All	All	All
Operating System	Linux	Linux Kernel	2.4.9	All	All	All
	cpe:2.3:o:linux:linux_kernel:2.4.0:*****:					
	cpe:2.3:o:linux:linux_kernel:2.4.1:*****:					
	cpe:2.3:o:linux:linux_kernel:2.4.10:*****:					
	cpe:2.3:o:linux:linux_kernel:2.4.11:*****:					
	cpe:2.3:o:linux:linux_kernel:2.4.12:*****:					
	cpe:2.3:o:linux:linux_kernel:2.4.13:*****:					
	cpe:2.3:o:linux:linux_kernel:2.4.14:*****:					
	cpe:2.3:o:linux:linux_kernel:2.4.15:*****:					
	cpe:2.3:o:linux:linux_kernel:2.4.16:*****:					
	cpe:2.3:o:linux:linux_kernel:2.4.17:*****:					
	cpe:2.3:o:linux:linux_kernel:2.4.18:*****:					
	cpe:2.3:o:linux:linux_kernel:2.4.19:*****:					
	cpe:2.3:o:linux:linux_kernel:2.4.2:*****:					
	cpe:2.3:o:linux:linux_kernel:2.4.20:*****:					
	cpe:2.3:o:linux:linux_kernel:2.4.21:*****:					
	cpe:2.3:o:linux:linux_kernel:2.4.22:*****:					
	cpe:2.3:o:linux:linux_kernel:2.4.23:*****:					
	cpe:2.3:o:linux:linux_kernel:2.4.24:*****:					
	cpe:2.3:o:linux:linux_kernel:2.4.3:*****:					
	cpe:2.3:o:linux:linux_kernel:2.4.4:*****:					
	cpe:2.3:o:linux:linux_kernel:2.4.5:*****:					
	cpe:2.3:o:linux:linux_kernel:2.4.6:*****:					
	cpe:2.3:o:linux:linux_kernel:2.4.7:*****:					
	cpe:2.3:o:linux:linux_kernel:2.4.8:*****:					

cpe:2.3:o:linux:linux_kernel:2.4.9:*****:
cpe:2.3:o:linux:linux_kernel:2.4.0:*****:
cpe:2.3:o:linux:linux_kernel:2.4.1:*****:
cpe:2.3:o:linux:linux_kernel:2.4.10:*****:
cpe:2.3:o:linux:linux_kernel:2.4.11:*****:
cpe:2.3:o:linux:linux_kernel:2.4.12:*****:
cpe:2.3:o:linux:linux_kernel:2.4.13:*****:
cpe:2.3:o:linux:linux_kernel:2.4.14:*****:
cpe:2.3:o:linux:linux_kernel:2.4.15:*****:
cpe:2.3:o:linux:linux_kernel:2.4.16:*****:
cpe:2.3:o:linux:linux_kernel:2.4.17:*****:
cpe:2.3:o:linux:linux_kernel:2.4.18:*****:
cpe:2.3:o:linux:linux_kernel:2.4.19:*****:
cpe:2.3:o:linux:linux_kernel:2.4.2:*****:
cpe:2.3:o:linux:linux_kernel:2.4.20:*****:
cpe:2.3:o:linux:linux_kernel:2.4.21:*****:
cpe:2.3:o:linux:linux_kernel:2.4.22:*****:
cpe:2.3:o:linux:linux_kernel:2.4.23:*****:
cpe:2.3:o:linux:linux_kernel:2.4.24:*****:
cpe:2.3:o:linux:linux_kernel:2.4.3:*****:
cpe:2.3:o:linux:linux_kernel:2.4.4:*****:
cpe:2.3:o:linux:linux_kernel:2.4.5:*****:
cpe:2.3:o:linux:linux_kernel:2.4.6:*****:
cpe:2.3:o:linux:linux_kernel:2.4.7:*****:
cpe:2.3:o:linux:linux_kernel:2.4.8:*****:
cpe:2.3:o:linux:linux_kernel:2.4.9:*****:

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](#)