



CVE-2003-0984

Published on: 12/23/2003 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:44 PM UTC

CVE-2003-0984

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

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

Real time clock (RTC) routines in Linux kernel 2.4.23 and earlier do not properly initialize their structures, which could leak kernel data to user space.

CVE-2003-0984 has been assigned by [M](#) cve@mitre.org 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

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

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

[DEBIAN DSA-1067](#)

Linux Kernel Real-time Clock Routines May Leak Kernel Data to User Applications - SecurityTracker

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

[SECTrack 1008594](#)

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

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

[DEBIAN DSA-1070](#)

Secunia - Advisories - SmoothWall Express update for kernel

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

[SECUNIA 10583](#)

Repository / Oval Repository

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

[OVAL oval:org.mitre.oval:def:1013](#)

NOVELL: Broken Link - 404 Error Pages	web.archive.org text/html Inactive Link Not Archived	 SUSE SuSE-SA:2003:049
Red Hat -- Linux, Embedded Linux and Open Source Solutions	www.redhat.com text/html	 FEDORA FEDORA-2003-046
Linux Kernel 2.4 RTC Handling Routines Memory Disclosure Vulnerability	Vendor Advisory cve.report (archive) text/html	 BID 9154
Secunia - Advisories - Mandrake update for kernel	web.archive.org text/html	 SECUNIA 10582
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:859
Debian -- Security Information -- DSA-1082-1 kernel-source-2.4.17	www.debian.org Deprecated Link text/html	 DEBIAN DSA-1082
Secunia - Advisories - Debian update for kernel-source-2.4.16	web.archive.org text/html	 SECUNIA 20162
Advisories - Mandriva	www.mandriva.com text/html	 MANDRAKE MDKSA-2004:001
Home - Conectiva	distro.conectiva.com.br text/html	 CONECTIVA CLA-2004:799
Secunia - Advisories - Debian update for kernel-source-2.4.18	web.archive.org text/html	 SECUNIA 20202
Secunia - Advisories - Linux Kernel Real Time Clock Kernel Memory Disclosure Vulnerability	web.archive.org text/html	 SECUNIA 10533
Secunia - Advisories - Red Hat update for kernel	web.archive.org text/html	 SECUNIA 10536
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:9406
LinuxSecurity.com: EnGarde: kernel bug and security fixes.	www.linuxsecurity.com text/html	 ENGARDE ESA-20040105-001
redhat.com Red Hat Support	Patch Vendor Advisory www.redhat.com text/html	 REDHAT RHSA-2004:188
Secunia - Advisories - Conectiva update for kernel	web.archive.org text/html	 SECUNIA 10537
Secunia - Advisories - Fedora update for kernel	web.archive.org text/html	 SECUNIA 10555
'SmoothWall Project Security Advisory SWP-2004:001' - MARC	marc.info text/html	 BUGTRAQ 20040112 SmoothWall Project Security Advisory SWP-2004:001
Secunia - Advisories - Debian update for kernel-source-2.4.17	web.archive.org text/html	 SECUNIA 20338
No Description Provided	www.osvdb.org Inactive Link Not Archived	 OSVDB 3317
redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2003:417

Secunia - Advisories - EnGarde update for kernel	web.archive.org text/html	 SECUNIA 10538
Debian -- Security Information -- DSA-1069-1 kernel-source-2.4.18	www.debian.org text/html Depreciated Link	 DEBIAN DSA-1069
Secunia - Advisories - Debian update for kernel-source-2.4.19	web.archive.org text/html	 SECUNIA 20163
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF linux-rtc-memory-leak(13943)

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
Operating System	Linux	Linux Kernel	2.4.0	test1	All	All
Operating System	Linux	Linux Kernel	2.4.0	test10	All	All
Operating System	Linux	Linux Kernel	2.4.0	test11	All	All
Operating System	Linux	Linux Kernel	2.4.0	test12	All	All
Operating System	Linux	Linux Kernel	2.4.0	test2	All	All
Operating System	Linux	Linux Kernel	2.4.0	test3	All	All
Operating System	Linux	Linux Kernel	2.4.0	test4	All	All
Operating System	Linux	Linux Kernel	2.4.0	test5	All	All
Operating System	Linux	Linux Kernel	2.4.0	test6	All	All
Operating System	Linux	Linux Kernel	2.4.0	test7	All	All
Operating System	Linux	Linux Kernel	2.4.0	test8	All	All
Operating System	Linux	Linux Kernel	2.4.0	test9	All	All
Operating	Linux	Linux Kernel	2.4.1	All	All	All

System						
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	2.4.18	All	x86	All
Operating System	Linux	Linux Kernel	2.4.18	pre1	All	All
Operating System	Linux	Linux Kernel	2.4.18	pre2	All	All
Operating System	Linux	Linux Kernel	2.4.18	pre3	All	All
Operating System	Linux	Linux Kernel	2.4.18	pre4	All	All
Operating System	Linux	Linux Kernel	2.4.18	pre5	All	All
Operating System	Linux	Linux Kernel	2.4.18	pre6	All	All
Operating System	Linux	Linux Kernel	2.4.18	pre7	All	All
Operating System	Linux	Linux Kernel	2.4.18	pre8	All	All
Operating System	Linux	Linux Kernel	2.4.19	All	All	All
Operating System	Linux	Linux Kernel	2.4.19	pre1	All	All
Operating System	Linux	Linux Kernel	2.4.19	pre2	All	All
Operating System	Linux	Linux Kernel	2.4.19	pre3	All	All
Operating	Linux	Linux Kernel	2.4.19	pre4	All	All

System						
Operating System	Linux	Linux Kernel	2.4.19	pre5	All	All
Operating System	Linux	Linux Kernel	2.4.19	pre6	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	2.4.21	pre1	All	All
Operating System	Linux	Linux Kernel	2.4.21	pre4	All	All
Operating System	Linux	Linux Kernel	2.4.21	pre7	All	All
Operating System	Linux	Linux Kernel	2.4.22	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
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	2.4.0	test1	All	All
Operating System	Linux	Linux Kernel	2.4.0	test10	All	All
Operating System	Linux	Linux Kernel	2.4.0	test11	All	All
Operating System	Linux	Linux Kernel	2.4.0	test12	All	All
Operating System	Linux	Linux Kernel	2.4.0	test2	All	All
Operating System	Linux	Linux Kernel	2.4.0	test3	All	All

Operating System	Linux	Linux Kernel	2.4.0	test4	All	All
Operating System	Linux	Linux Kernel	2.4.0	test4	All	All
Operating System	Linux	Linux Kernel	2.4.0	test5	All	All
Operating System	Linux	Linux Kernel	2.4.0	test6	All	All
Operating System	Linux	Linux Kernel	2.4.0	test7	All	All
Operating System	Linux	Linux Kernel	2.4.0	test8	All	All
Operating System	Linux	Linux Kernel	2.4.0	test9	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	2.4.18	All	x86	All
Operating System	Linux	Linux Kernel	2.4.18	pre1	All	All
Operating System	Linux	Linux Kernel	2.4.18	pre2	All	All
Operating System	Linux	Linux Kernel	2.4.18	pre3	All	All
Operating System	Linux	Linux Kernel	2.4.18	pre4	All	All
Operating System	Linux	Linux Kernel	2.4.18	pre5	All	All
Operating System	Linux	Linux Kernel	2.4.18	pre6	All	All

Operating System	Linux	Linux Kernel	2.4.18	pre0	All	All
Operating System	Linux	Linux Kernel	2.4.18	pre7	All	All
Operating System	Linux	Linux Kernel	2.4.18	pre8	All	All
Operating System	Linux	Linux Kernel	2.4.19	All	All	All
Operating System	Linux	Linux Kernel	2.4.19	pre1	All	All
Operating System	Linux	Linux Kernel	2.4.19	pre2	All	All
Operating System	Linux	Linux Kernel	2.4.19	pre3	All	All
Operating System	Linux	Linux Kernel	2.4.19	pre4	All	All
Operating System	Linux	Linux Kernel	2.4.19	pre5	All	All
Operating System	Linux	Linux Kernel	2.4.19	pre6	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	2.4.21	pre1	All	All
Operating System	Linux	Linux Kernel	2.4.21	pre4	All	All
Operating System	Linux	Linux Kernel	2.4.21	pre7	All	All
Operating System	Linux	Linux Kernel	2.4.22	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
Operating System	Linux	Linux Kernel	2.4.9	All	All	All

cpe:2.3:o:linux:linux_kernel:2.4.18:pre4:*****:
cpe:2.3:o:linux:linux_kernel:2.4.18:pre5:*****:
cpe:2.3:o:linux:linux_kernel:2.4.18:pre6:*****:
cpe:2.3:o:linux:linux_kernel:2.4.18:pre7:*****:
cpe:2.3:o:linux:linux_kernel:2.4.18:pre8:*****:
cpe:2.3:o:linux:linux_kernel:2.4.19:*****:
cpe:2.3:o:linux:linux_kernel:2.4.19:pre1:*****:
cpe:2.3:o:linux:linux_kernel:2.4.19:pre2:*****:
cpe:2.3:o:linux:linux_kernel:2.4.19:pre3:*****:
cpe:2.3:o:linux:linux_kernel:2.4.19:pre4:*****:
cpe:2.3:o:linux:linux_kernel:2.4.19:pre5:*****:
cpe:2.3:o:linux:linux_kernel:2.4.19:pre6:*****:
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:2.4.21:pre1:*****:
cpe:2.3:o:linux:linux_kernel:2.4.21:pre4:*****:
cpe:2.3:o:linux:linux_kernel:2.4.21:pre7:*****:
cpe:2.3:o:linux:linux_kernel:2.4.22:*****:
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:2.4.0:test1:*****:
cpe:2.3:o:linux:linux_kernel:2.4.0:test10:*****:

cpe:2.3:o:linux:linux_kernel:2.4.0:test11:~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.4.0:test12:~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.4.0:test2:~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.4.0:test3:~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.4.0:test4:~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.4.0:test5:~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.4.0:test6:~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.4.0:test7:~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.4.0:test8:~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.4.0:test9:~::~~::~~::~~:::
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:2.4.18:*:x86:~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.4.18:pre1:~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.4.18:pre2:~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.4.18:pre3:~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.4.18:pre4:~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.4.18:pre5:~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.4.18:pre6:~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.4.18:pre7:~::~~::~~::~~:::

cpe:2.3:o:linux:linux_kernel:2.4.18:pre8:*****:
cpe:2.3:o:linux:linux_kernel:2.4.19:*****:
cpe:2.3:o:linux:linux_kernel:2.4.19:pre1:*****:
cpe:2.3:o:linux:linux_kernel:2.4.19:pre2:*****:
cpe:2.3:o:linux:linux_kernel:2.4.19:pre3:*****:
cpe:2.3:o:linux:linux_kernel:2.4.19:pre4:*****:
cpe:2.3:o:linux:linux_kernel:2.4.19:pre5:*****:
cpe:2.3:o:linux:linux_kernel:2.4.19:pre6:*****:
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:2.4.21:pre1:*****:
cpe:2.3:o:linux:linux_kernel:2.4.21:pre4:*****:
cpe:2.3:o:linux:linux_kernel:2.4.21:pre7:*****:
cpe:2.3:o:linux:linux_kernel:2.4.22:*****:
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

[← Previous ID](#)

[Next ID →](#)

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](#)