



CVE-2002-1571

Published on: 12/31/2002 05:00:00 AM UTC

Last Modified on: 06/15/2021 12:00:00 AM UTC

CVE-2002-1571

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

The linux 2.4 kernel before 2.4.19 assumes that the frinit instruction clears all registers, which could lead to an information leak on processors that do not clear all relevant SSE registers.

CVE-2002-1571 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **2.1 - LOW**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

404 Not Found

[search.luky.org](#)

[text/html](#)

Inactive Link Not Archived

[MLIST \[linux-kernel\] 20020418 Re: SSE related security hole](#)

No Description Provided

[linux.bkbits.net](#)

Inactive Link Not Archived

[CONFIRM linux.bkbits.net:8080/linux-2.4/diffs/arch/i386/kernel/i387.c@1.6](#)

Linux-kernel mailing list archive 2002-15,: SSE related security hole

[www.cs.helsinki.fi](#)

[text/x-c](#)

[MLIST \[linux-kernel\] 20020417 SSE related security hole](#)

RE: SSE related security hole

[web.archive.org](#)

[text/html](#)

Inactive Link Not Archived

[MLIST \[linux-kernel\] 20020422 Re: SSE related security hole](#)

Linux-kernel mailing list archive 2002-15,: Re: SSE related security hole

[www.cs.helsinki.fi](#)

[text/html](#)

[MLIST \[linux-kernel\] 20020417 Re: SSE related security hole](#)

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 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

System						
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 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	2.4.3	All	All	All

System						
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	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	Linux	Linux Kernel	2.4.12	All	All	All

System						
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 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	Linux	Linux Kernel	2.4.2	All	All	All

System						
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:2.4.0:****:*:*:						
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:2.4.3:****:*:
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:****:*:

УРЕ.З.У.У.ИИИУА.ИИИУА_КЕИИЕИ.З.Т.У.

```
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:2.4.3:*****:
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.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](#)