



CVE-2005-3847

Published on: 11/26/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:22 PM UTC

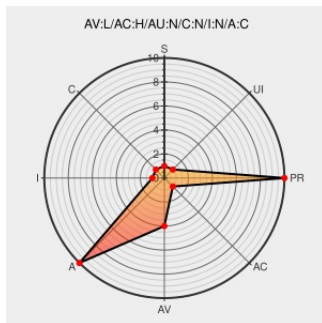
CVE-2005-3847

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

The `handle_stop_signal` function in `signal.c` in Linux kernel 2.6.11 up to other versions before 2.6.13 and 2.6.12.6 allows local users to cause a denial of service (deadlock) by sending a SIGKILL to a real-time threaded process while it is performing a core dump.

CVE-2005-3847 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

HIGH

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

'[PATCH 2.6.12.5] NPTL
signal delivery deadlock
fix' - MARC

[marc.info](#)
[text/x-diff](#)

[MLIST \[linux-kernel\] 20050817 \[PATCH 2.6.12.5\] NPTL signal delivery deadlock f](#)

Debian update for kernel-
source-2.6.8 - Advisories
- Secunia

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

[SECUNIA 19374](#)

SuSE Security
announcements: [suse-
security-announce] SUSE
Security Announcement:
kernel various security
problems (SUSE-
SA:2006:012)

[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[SUSE SUSE-SA:2006:012](#)

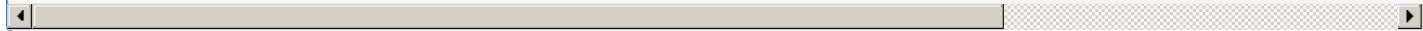
'[PATCH 2/7] [PATCH]

[marc.info](#)

[MLIST \[linux-kernel\] 20050826 \[PATCH 2/7\] \[PATCH\] NPTL signal delivery deadl](#)

kernel/git/torvalds/linux.git - Linux kernel source tree	Patch www.kernel.org text/html	CONFIRM www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=dd12f48d4e8774415b528d3991ae47c28f26e1ac;hp=ade6648
Secunia - Advisories - SUSE update for kernel	Vendor Advisory web.archive.org text/html	SECUNIA 19038
No Description Provided	Patch www.kernel.org text/html Inactive Link Not Archived	CONFIRM www.kernel.org/git/?p=linux/kernel/git/chrisw/stable-queue.git;a=blob;h=f6cc7e101c49f356e4c4df5cca1ff352a0f01dd5;hb=9c5fcb99af7c1signal-delivery-deadlock-fix.patch
Linux Kernel handle_stop_signal Denial of Service Vulnerability	cve.report (archive) text/html	BID 16856
Debian -- Security Information -- DSA-1017-1 kernel-source-2.6.8	Patch Vendor Advisory www.debian.org Deprecated Link text/html	DEBIAN DSA-1017

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	2.6.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.5	All	All	All

System						
Operating System	Linux	Linux Kernel	2.6.11.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.12.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc5	All	All

System						
Operating System	Linux	Linux Kernel	2.6.13	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc7	All	All
Operating System	Linux	Linux Kernel	2.6.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.10	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.11	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.8	All	All	All
Operating System	Linux	Linux Kernel	2.6.11.9	All	All	All
Operating System	Linux	Linux Kernel	2.6.12	All	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.12	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.12.1	All	All	All

Operating System	Linux	Linux Kernel	2.6.12.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.12.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.13	All	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.13	rc7	All	All
cpe:2.3:o:linux:linux_kernel:2.6.11:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.11.1:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.11.10:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.11.11:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.11.12:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.11.2:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.11.3:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.11.4:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.11.5:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.11.6:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.11.7:*:*:*:*:*:						
cpe:2.3:o:linux:linux_kernel:2.6.11.8:*:*:*:*:*:						

```
cpu:2.3.0:linux:linux_kernel:2.6.11.8: : : : : :
```

```
cpe:2.3:o:linux:linux_kernel:2.6.11.9:*:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux kernel:2.6.12:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.12:rc1:::~::~:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.12:rc2:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.12:rc3:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.12:rc4:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.12:rc5:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.12:rc6:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.12.1:::*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.12.2:::~::~:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.12.3:*:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.12.4:::~::~:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.12.5:::~::~:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.12.6:*:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.13:*:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.13:rc1:::*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.13:rc2:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.13:rc3:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.13:rc4:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux kernel:2.6.13:rc5:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux kernel:2.6.13:rc6:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux kernel:2.6.13:rc7:::~::~:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.11:.*:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:o:linux:linux kernel:2.6.11.1:::~::~:
```

```
cpe:2.3:o:linux:linux kernel:2.6.11.10:*.:*:*:*:*.*
```

```
cpe:2.3:o:linux:linux_kernel:2.6.11.11:*.:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.11.12:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux kernel:2.6.11.2:*:*:*:*:*:
```

cpe:2.3:o:linux:linux_kernel:2.6.11.3:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.11.4:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.11.5:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.11.6:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.11.7:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.11.8:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.11.9:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.12:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.12:rc1:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.12:rc2:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.12:rc3:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.12:rc4:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.12:rc5:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.12:rc6:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.12.1:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.12.2:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.12.3:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.12.4:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.12.5:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.12.6:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.13:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.13:rc1:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.13:rc2:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.13:rc3:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.13:rc4:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.13:rc5:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.13:rc6:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.13:rc7:~::~~::~~::~~::~~::~~::~~:::

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](#)