

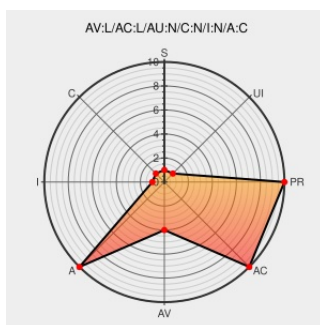


CVE-2006-1055

Published on: 04/05/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:00 PM UTC

CVE-2006-1055

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

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

The fill_write_buffer function in sysfs/file.c in Linux kernel 2.6.12 up to versions before 2.6.17-rc1 does not zero terminate a buffer when a length of PAGE_SIZE or more is requested, which might allow local users to cause a denial of service (crash) by causing an out-of-bounds read.

CVE-2006-1055 has been assigned by secalert@redhat.com 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

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

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

[VUPEN ADV-2006-1273](#)

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=commit;h=6e0dd741a89be35defa05bd79f4211c5a2762825

LWN: Fedora alert
FEDORA-2006-423
(kernel)

lwn.net
[text/html](#)

[FEDORA FEDORA-2006-423](#)

Ubuntu update for kernel
- Advisories - Secunia

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

[SECUNIA 20716](#)

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2006-1475
Fedora update for kernel - Advisories - Secunia	web.archive.org text/html	SECUNIA 19735
USN-281-1: Linux kernel vulnerabilities Ubuntu security notices	usn.ubuntu.com text/html	UBUNTU USN-281-1
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 24443
Secunia - Advisories - Ubuntu update for kernel	web.archive.org text/html	SECUNIA 19955
usn/usn-302-1 - Ubuntu: Linux for human beings	www.ubuntu.com text/html	UBUNTU USN-302-1
Linux Kernel SYSFS Local Denial of Service Vulnerability - Advisories - Secunia	web.archive.org text/html	SECUNIA 19495
	www.trustix.org text/plain Inactive Link Not Archived	TRUSTIX 2006-0020
Security Announcement	web.archive.org text/html Inactive Link Not Archived	SUSE SUSE-SA:2006:028
Linux Kernel SYSFS PAGE_SIZE Local Denial of Service Vulnerability	cve.report (archive) text/html	BID 17402
kernel/git/torvalds/linux.git - Linux kernel source tree	Exploit Patch www.kernel.org text/html	CONFIRM www.kernel.org/git/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commitdiff;h=6e0dd741a89be35defa05bd79f4211c5a2762825;hp=597a7
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF linux-fillwritebuffer-dos(25693)
SUSE update for kernel - Advisories - Secunia	web.archive.org text/html	SECUNIA 20398

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	2.6.12	All	All	All

System						
Operating System	Linux	Linux Kernel	2.6.12	rc1	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	2.6.12.1	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	rc4	All	All
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	2.6.13.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.13.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.13.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.13.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.14	All	All	All
Operating System	Linux	Linux Kernel	2.6.14	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.14	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.14	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.14	rc4	All	All

System						
Operating System	Linux	Linux Kernel	2.6.14.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.15	All	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc7	All	All
Operating System	Linux	Linux Kernel	2.6.15.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.15.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.15.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.15.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.15.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.16	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.17	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	rc4	All	All
Operating	Linux	Linux Kernel	2.6.12	rc5	All	All

System						
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	rc4	All	All
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	2.6.13.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.13.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.13.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.13.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.14	All	All	All
Operating System	Linux	Linux Kernel	2.6.14	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.14	rc2	All	All
Operating System	Linux	Linux Kernel	2.6.14	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.14	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.14.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.2	All	All	All
Operating	Linux	Linux Kernel	2.6.14.3	All	All	All

System						
Operating System	Linux	Linux Kernel	2.6.14.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.14.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.15	All	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc3	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc4	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc5	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc6	All	All
Operating System	Linux	Linux Kernel	2.6.15	rc7	All	All
Operating System	Linux	Linux Kernel	2.6.15.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.15.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.15.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.15.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.15.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.16	rc1	All	All
Operating System	Linux	Linux Kernel	2.6.17	All	All	All
	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:rc4:*****:					
	cpe:2.3:o:linux:linux_kernel:2.6.12:rc5:*****:					
	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:rc4:~::~~::~~::~~::~~::~~::~~:::
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:2.6.13.1:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.13.2:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.13.3:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.13.4:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.14:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.14:rc1:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.14:rc2:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.14:rc3:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.14:rc4:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.14.1:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.14.2:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.14.3:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.14.4:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.14.5:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.15:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.15:rc1:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.15:rc3:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.15:rc4:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.15:rc5:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.15:rc6:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:o:linux:linux_kernel:2.6.15:rc7:~::~~::~~::~~::~~::~~::~~:::

```
cpe:2.3:o:linux:linux_kernel:2.6.15.1:*:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.15.2:*:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.15.3:*:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.15.4:*:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.15.5:*:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.16:rc1:::*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.17:*:*:*:*:*:*:
```

```
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:rc4:*:*:*:*:*:
```

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

```
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:rc4:*:*:*:*:*:
```

```
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:2.6.13.1:::~::~:
```

```
cpe:2.3:o:linux:linux kernel:2.6.13.2:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux_kernel:2.6.13.3:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux kernel:2.6.13.4:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux kernel:2.6.14:*.:*:*:*:*.*
```

```
cpe:2.3:o:linux:linux kernel:2.6.14:rc1:*:*:*:*:*:
```

```
cpe:2.3:o:linux:linux kernel:2.6.14:rc2:*:*:*:*:*:
```

cpe:2.3:o:linux:linux_kernel:2.6.14:rc3:~::~~::~~::~~::~~::~~::
cpe:2.3:o:linux:linux_kernel:2.6.14:rc4:~::~~::~~::~~::~~::~~::
cpe:2.3:o:linux:linux_kernel:2.6.14.1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:linux:linux_kernel:2.6.14.2:~::~~::~~::~~::~~::~~::
cpe:2.3:o:linux:linux_kernel:2.6.14.3:~::~~::~~::~~::~~::~~::
cpe:2.3:o:linux:linux_kernel:2.6.14.4:~::~~::~~::~~::~~::~~::
cpe:2.3:o:linux:linux_kernel:2.6.14.5:~::~~::~~::~~::~~::~~::
cpe:2.3:o:linux:linux_kernel:2.6.15:~::~~::~~::~~::~~::~~::
cpe:2.3:o:linux:linux_kernel:2.6.15:rc1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:linux:linux_kernel:2.6.15:rc3:~::~~::~~::~~::~~::~~::
cpe:2.3:o:linux:linux_kernel:2.6.15:rc4:~::~~::~~::~~::~~::~~::
cpe:2.3:o:linux:linux_kernel:2.6.15:rc5:~::~~::~~::~~::~~::~~::
cpe:2.3:o:linux:linux_kernel:2.6.15:rc6:~::~~::~~::~~::~~::~~::
cpe:2.3:o:linux:linux_kernel:2.6.15:rc7:~::~~::~~::~~::~~::~~::
cpe:2.3:o:linux:linux_kernel:2.6.15.1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:linux:linux_kernel:2.6.15.2:~::~~::~~::~~::~~::~~::
cpe:2.3:o:linux:linux_kernel:2.6.15.3:~::~~::~~::~~::~~::~~::
cpe:2.3:o:linux:linux_kernel:2.6.15.4:~::~~::~~::~~::~~::~~::
cpe:2.3:o:linux:linux_kernel:2.6.15.5:~::~~::~~::~~::~~::~~::
cpe:2.3:o:linux:linux_kernel:2.6.16:rc1:~::~~::~~::~~::~~::~~::
cpe:2.3:o:linux:linux_kernel:2.6.17:~::~~::~~::~~::~~::~~::

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

[site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report