

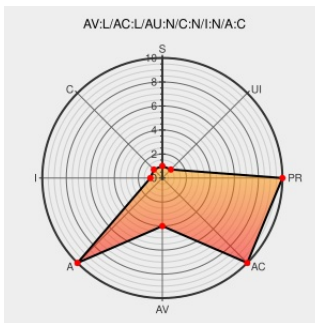


CVE-2006-7051

Published on: 02/23/2007 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:01 PM UTC

CVE-2006-7051

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

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

The `sys_timer_create` function in `posix-timers.c` for Linux kernel 2.6.x allows local users to cause a denial of service (memory consumption) and possibly bypass memory limits or cause other processes to be killed by creating a large number of posix timers, which are allocated in kernel memory but are not treated as part of the process' memory.

CVE-2006-7051 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

CXSecurity - IDS

[securityreason.com](#)
[text/html](#)

[SREASON 2287](#)

SecurityFocus

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

[BUGTRAQ 20060404 Linux Kernel Local DoS vulnerability.](#)

Linux Kernel 2.6.x - 'sys_timer_create()' Local Denial of Service - Linux dos Exploit

[www.exploit-db.com](#)
[Proof of Concept](#)
[text/html](#)

[EXPLOIT-DB 1657](#)

IBM X-Force Exchange

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

[XF linux-systimercreate-dos\(25712\)](#)

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	2.6.18.0	All	All	All
Operating System	Linux	Linux Kernel	2.6.18.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.18.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.18.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.18.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.18.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.18.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.18.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.19	All	All	All
Operating System	Linux	Linux Kernel	2.6.19.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.19.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.19.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.19.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.20	All	All	All
Operating System	Linux	Linux Kernel	2.6.20.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.18.0	All	All	All
Operating System	Linux	Linux Kernel	2.6.18.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.18.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.18.3	All	All	All

Operating System	Linux	Linux Kernel	2.6.18.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.18.5	All	All	All
Operating System	Linux	Linux Kernel	2.6.18.6	All	All	All
Operating System	Linux	Linux Kernel	2.6.18.7	All	All	All
Operating System	Linux	Linux Kernel	2.6.19	All	All	All
Operating System	Linux	Linux Kernel	2.6.19.1	All	All	All
Operating System	Linux	Linux Kernel	2.6.19.2	All	All	All
Operating System	Linux	Linux Kernel	2.6.19.3	All	All	All
Operating System	Linux	Linux Kernel	2.6.19.4	All	All	All
Operating System	Linux	Linux Kernel	2.6.20	All	All	All
Operating System	Linux	Linux Kernel	2.6.20.1	All	All	All
cpe:2.3:o:linux:linux_kernel:2.6.18.0:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.18.1:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.18.2:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.18.3:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.18.4:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.18.5:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.18.6:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.18.7:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.19:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.19.1:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.19.2:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.19.3:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.19.4:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.20:*****:						
cpe:2.3:o:linux:linux_kernel:2.6.20.1:*****:						

cpe:2.3:o:linux:linux_kernel:2.6.18.0:*****:
cpe:2.3:o:linux:linux_kernel:2.6.18.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.18.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.18.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.18.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.18.5:*****:
cpe:2.3:o:linux:linux_kernel:2.6.18.6:*****:
cpe:2.3:o:linux:linux_kernel:2.6.18.7:*****:
cpe:2.3:o:linux:linux_kernel:2.6.19:*****:
cpe:2.3:o:linux:linux_kernel:2.6.19.1:*****:
cpe:2.3:o:linux:linux_kernel:2.6.19.2:*****:
cpe:2.3:o:linux:linux_kernel:2.6.19.3:*****:
cpe:2.3:o:linux:linux_kernel:2.6.19.4:*****:
cpe:2.3:o:linux:linux_kernel:2.6.20:*****:
cpe:2.3:o:linux:linux_kernel:2.6.20.1:*****: