

[Full-Disclosure] [GLSA 200407-02] Linux Kernel: Multiple vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-07/0209.html>

From: Tim Yamin (plasmaroo_at_gentoo.org)

Date: 07/04/04

To: gentoo-announce@gentoo.org

Date: Sat, 03 Jul 2004 23:53:18 +0100

Gentoo Linux Security Advisory GLSA 200407-02

<http://security.gentoo.org/>

Severity: High

Title: Linux Kernel: Multiple vulnerabilities

Date: July 03, 2004

Bugs: #47881, #49637, #53804, #54976, #55698

ID: 200407-02

Synopsis
=====

Multiple vulnerabilities have been found in the Linux kernel used by GNU/Linux systems. Patched, or updated versions of these kernels have been released and details are included in this advisory.

Background
=====

The Linux kernel is responsible for managing the core aspects of a GNU/Linux system, providing an interface for core system applications as well as providing the essential structure and capability to access hardware that is needed for a running system.

Affected packages
=====

Kernel / Unaffected / Rmerge

-
- 1 aa-sources == 2.4.23-r2 YES
 - 2 alpha-sources >= 2.4.21-r8
 - 3 ck-sources == 2.4.26-r1 YES
 - >= 2.6.7-r1 YES
 - 4 compaq-sources >= 2.4.9.32.7-r7
 - 5 development-sources >= 2.6.7
 - 6 gaming-sources >= 2.4.20-r14
 - 7 gentoo-dev-sources >= 2.6.7
 - 8 gentoo-sources *>= 2.4.19-r17
 - *>= 2.4.20-r20
 - *>= 2.4.22-r12
 - *>= 2.4.25-r5
 - >= 2.4.26-r3
 - 9 grsec-sources >= 2.4.26.2.0-r5
 - 10 gs-sources >= 2.4.25_pre7-r7
 - 11 hardened-dev-sources >= 2.6.7
 - 12 hardened-sources >= 2.4.26-r2
 - 13 hppa-dev-sources >= 2.6.7
 - 14 hppa-sources >= 2.4.26_p6
 - 15 ia64-sources >= 2.4.24-r5
 - 16 mips-sources >= 2.4.26-r3
 - 17 mm-sources >= 2.6.7-r1
 - 18 openmosix-sources >= 2.4.22-r10
 - 19 pac-sources >= 2.4.23-r8
 - 20 pegasos-dev-sources >= 2.6.7
 - 21 pegasos-sources >= 2.4.26-r2
 - 22 planet-crma-sources >= 2.4.21-r10
 - 23 ppc-sources >= 2.4.26-r2
 - 24 ppc64-sources >= 2.6.7
 - 25 rsbac-sources >= 2.4.26-r2
 - 26 rsbac-dev-sources >= 2.6.7-r1
 - 27 selinux-sources >= 2.4.26-r2
 - 28 sparc-sources >= 2.4.26-r2
 - 29 uclinux-sources >= 2.4.26_p0-r2
 - 30 usermode-sources *>= 2.4.24-r5
 - >= 2.4.26-r2
 - 31 vanilla-sources Vulnerable!
 - 32 vserver-sources >= 2.4.26.1.3.9-r2
 - 33 win4lin-sources >= 2.4.26-r2
 - 34 wolk-sources *>= 4.9-r9
 - *>= 4.11-r6
 - >= 4.14-r3
 - 35 xbox-sources >= 2.6.7
 - 36 xfs-sources >= 2.4.24-r8

NOTE: Some kernels are still vulnerable. Users should migrate to another kernel if one is available or seek another solution such as patching their existing kernel.

NOTE: Packages marked with "Remerge" as "YES" require a re-merge

even though Portage does not indicate a newer version!

36 affected packages on all of their supported architectures.

Description

Multiple flaws have been discovered in the Linux kernel. This advisory corrects the following issues:

- * CAN-2004-0109: This vulnerability allows privilege escalation using ISO9660 file systems through a buffer overflow via a malformed file system containing a long symbolic link entry. This can allow arbitrary code execution at kernel level.
- * CAN-2004-0133: The XFS file system in 2.4 series kernels has an information leak by which data in the memory can be written to the device hosting the file system, allowing users to obtain portions of kernel memory by reading the raw block device.
- * CAN-2004-0177: The ext3 file system in 2.4 series kernels does not properly initialize journal descriptor blocks, causing an information leak by which data in the memory can be written to the device hosting the file system, allowing users to obtain portions of kernel memory by reading the raw device.
- * CAN-2004-0181: The JFS file system in 2.4 series kernels has an information leak by which data in the memory can be written to the device hosting the file system, allowing users to obtain portions of kernel memory by reading the raw device.
- * CAN-2004-0178: The OSS Sound Blaster [R] Driver has a Denial of Service vulnerability since it does not handle certain sample sizes properly. This allows local users to hang the kernel.
- * CAN-2004-0228: Due to an integer signedness error in the CPUFreq /proc handler code in 2.6 series Linux kernels, local users can escalate their privileges.
- * CAN-2004-0229: The framebuffer driver in 2.6 series kernel drivers does not use the fb_copy_cmap method of copying structures. The impact of this issue is unknown, however.
- * CAN-2004-0394: A buffer overflow in the panic() function of 2.4 series Linux kernels exists, but it may not be exploitable under normal circumstances due to its functionality.
- * CAN-2004-0427: The do_fork() function in both 2.4 and 2.6 series Linux kernels does not properly decrement the mm_count counter when an error occurs, triggering a memory leak that allows local users to

Full-Disclosure: [Full-Disclosure] [GLSA 200407-02] Linux Kernel: Multiple vulnerabilities

cause a Denial of Service by exhausting other applications of memory; causing the kernel to panic or to kill services.

- * CAN-2004-0495: Multiple vulnerabilities found by the Sparse source checker in the kernel allow local users to escalate their privileges or gain access to kernel memory.
- * CAN-2004-0535: The e1000 NIC driver does not properly initialize memory structures before using them, allowing users to read kernel memory.
- * CAN-2004-0554: 2.4 and 2.6 series kernels running on an x86 or an AMD64 architecture allow local users to cause a Denial of Service by a total system hang, due to an infinite loop that triggers a signal handler with a certain sequence of fsave and frstor instructions.
- * Local DoS in PaX: If ASLR is enabled as a GRSecurity PaX feature, a Denial of Service can be achieved by putting the kernel into an infinite loop. Only 2.6 series GRSecurity kernels are affected by this issue.
- * RSBAC 1.2.3 JAIL issues: A flaw in the RSBAC JAIL implementation allows suid/sgid files to be created inside the jail since the relevant module does not check the corresponding mode values. This can allow privilege escalation inside the jail. Only rsbac-(dev-)sources are affected by this issue.

Impact

=====

Arbitrary code with normal non-super-user privileges may be able to exploit any of these vulnerabilities; gaining kernel level access to memory structures and hardware devices. This may be used for further exploitation of the system, to leak sensitive data or to cause a Denial of Service on the affected kernel.

Workaround

=====

Although users may not be affected by certain vulnerabilities, all kernels are affected by the CAN-2004-0394, CAN-2004-0427 and CAN-2004-0554 issues which have no workaround. As a result, all users are urged to upgrade their kernels to patched versions.

Resolution

=====

Users are encouraged to upgrade to the latest available sources for their system:

Full-Disclosure: [Full-Disclosure] [GLSA 200407-02] Linux Kernel: Multiple vulnerabilities

```
# emerge sync
# emerge -pv your-favorite-sources
# emerge your-favorite-sources

## Follow usual procedure for compiling and installing a kernel.
## If you use genkernel, run genkernel as you would do normally.
```

Availability

=====

This GLSA and any updates to it are available for viewing at the Gentoo Security Website:

<http://security.gentoo.org/glsa/glsa-200407-02.xml>

Concerns?

=====

Security is a primary focus of Gentoo Linux and ensuring the confidentiality and security of our users machines is of utmost importance to us. Any security concerns should be addressed to security@gentoo.org or alternatively, you may file a bug at <http://bugs.gentoo.org>.

License

=====

Copyright 2004 Gentoo Technologies, Inc; referenced text belongs to its owner(s).

The contents of this document are licensed under the Creative Commons – Attribution / Share Alike license.

<http://creativecommons.org/licenses/by-sa/1.0>

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>

- application/pgp-signature attachment: [OpenPGP digital signature](#)