JSSI 2013

Veille avancée sur le noyau Linux

Etienne Comet

19/03/2013

Sommaire

- **Analyser un CVE noyau**
- **Chercher les bugs corrigés silencieusement**
- **Le GIT**
- **Pousser l'analyse d'un bug : étudier son exploitabilité**

Introduction

- **Contexte**
  - Pénurie d'exploits publics
- **Objectif**
  - Elever ses privilèges
- **Problématiques :**
  - De nombreuses informations à examiner
  - Des informations peu détaillées
  - Beaucoup de bugs corrigés silencieusement
  - De nombreux bugs inutiles

Analyser un CVE noyau

National Cyber-Alert System

Vulnerability Summary for CVE-2012-3552

Original release date: 10/03/2012

Last revised: 01/24/2013

Source: US-CERT/NIST

Overview

Race condition in the IP implementation in the Linux kernel before 3.0 might allow remote attackers to cause a denial of service (slab corruption and system crash) by sending packets to an application that sets socket options during the handling of network traffic.

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 5.4 (MEDIUM) (AV:N/AC:H/Au:N/C:N/I:N/A:C) (legend)

Impact Subscore: 6.9

Exploitability Subscore: 4.9

CVSS Version 2 Metrics:

Access Vector: Network exploitable

Access Complexity: High

Authentication: Not required to exploit

Impact Type: Allows disruption of serviceUnknown

Analyser un CVE noyau

External Source : CONFIRM

Name: http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=f6d8bd051c391c1c0458a30b2a7abcd939329259

Type: Patch Information

Hyperlink: http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=f6d8bd051c391c1c0458a30b2a7abcd939329259

External Source : CONFIRM

Name: https://github.com/torvalds/linux/commit/f6d8bd051c391c1c0458a30b2a7abcd939329259

Hyperlink: https://github.com/torvalds/linux/commit/f6d8bd051c391c1c0458a30b2a7abcd939329259

External Source : CONFIRM

Name: https://bugzilla.redhat.com/show_bug.cgi?id=853465

Hyperlink: https://bugzilla.redhat.com/show_bug.cgi?id=853465

External Source : MLIST

Name: [oss-security] 20120831 Re: CVE Request -- kernel: net: slab corruption due to improper synchronization around inet->opt

Hyperlink: http://www.openwall.com/lists/oss-security/2012/08/31/11

External Source : REDHAT

Name: RHSA-2012:1540

Hyperlink: http://rhn.redhat.com/errata/RHSA-2012-1540.html

External Source : CONFIRM

Name: http://ftp.osuosl.org/pub/linux/kernel/v3.0/ChangeLog-3.0

Hyperlink: http://ftp.osuosl.org/pub/linux/kernel/v3.0/ChangeLog-3.0

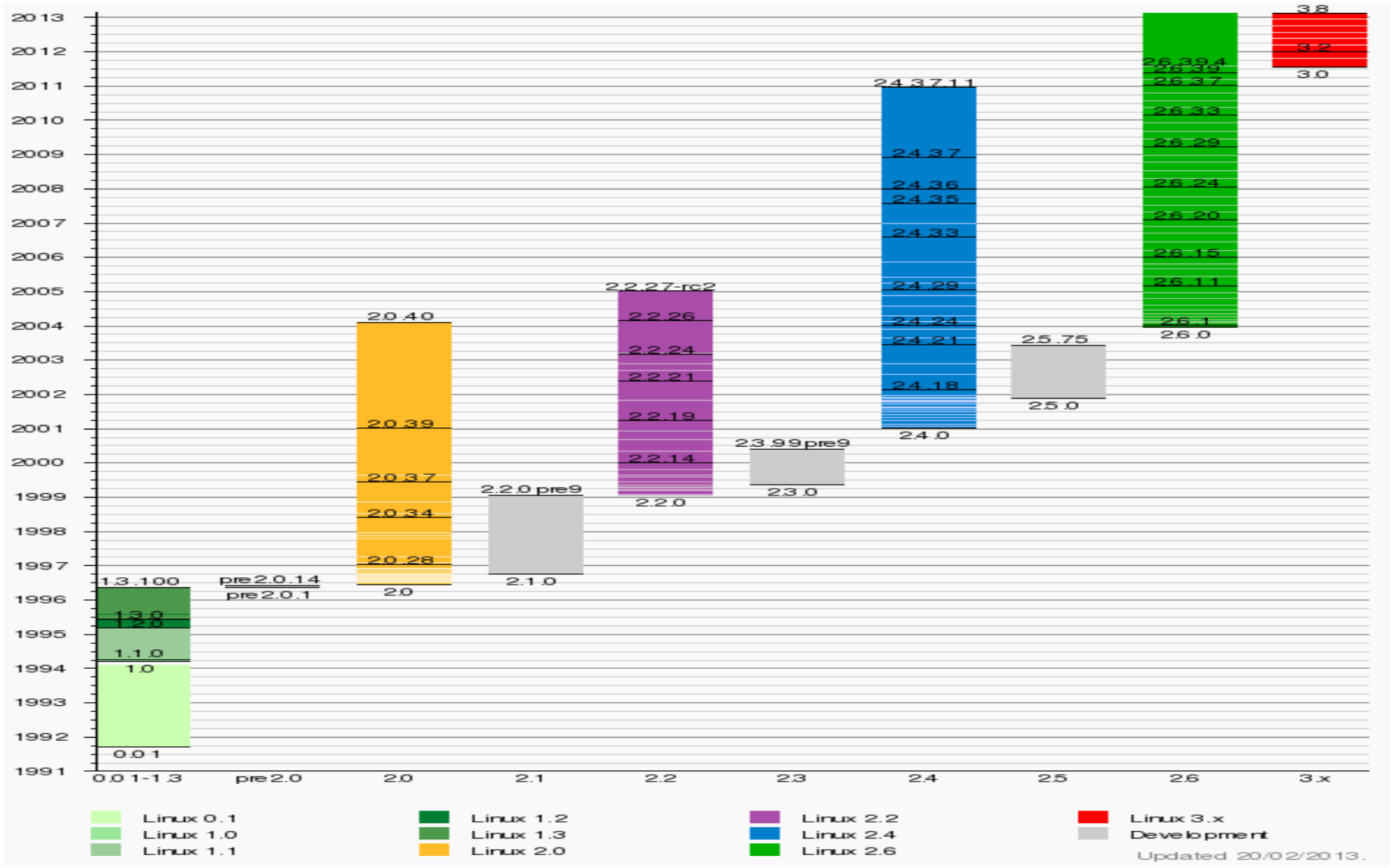
Analyser un CVE noyau

- **Les éléments importants**
  - Nature du bug
  - Conséquences du bug
  - Versions affectées
  - Partie du noyau affectée
  - Configuration nécessaire
  - Complexité d'exploitation

Analyser un CVE noyau

- **Différents types de bugs**
  - Integer overflows (CVE-2010-3442)
  - Bugs de signe (CVE-2010-3437)
  - Buffer overflows (CVE-2010-1084)
  - Double free (CVE-2011-1479)
  - Reuse after free (CVE-2009-4141 : fasync)
  - Mauvaises vérifications de droits (CVE-2010-4347)
  - Race conditions (CVE-2012-3552)
  - Leak d'informations (CVE-2011-2495)
  - Dead locks, infinite loop et bien d'autres...

Analyser un CVE noyau



Analyser un CVE noyau

Kernel series	Original release date	Current version
2.0	June 9, 1996	2.0.40[104]
2.2	January 26, 1999	2.2.26[106]
2.4	January 4, 2001	2.4.37.11
2.6.16	March 20, 2006	2.6.16.62
2.6.27	October 9, 2008	2.6.27.62[111]
2.6.32	December 3, 2009	2.6.32.60[113]
2.6.33	February 24, 2010	2.6.33.20[111]
2.6.34	May 16, 2010	2.6.34.14[111]
2.6.35	August 1, 2010	2.6.35.14[119]
2.6.38	March 15, 2011	2.6.38.8[111]
2.6.39	May 19, 2011	2.6.39.4[111]
3.0	July 22, 2011	3.0.66[120]
3.1	October 24, 2011	3.1.10
3.2	January 4, 2012	3.2.39
3.3	March 18, 2012	3.3.8
3.4	May 20, 2012	3.4.33[122]
3.5	July 21, 2012	3.5.7
3.6	September 30, 2012	3.6.11
3.7	December 11, 2012	3.7.9[126]
3.8	February 18, 2013	3.8[126]

Analyser un CVE noyau

- **CVE-2012-3400**

> Heap-based buffer overflow in the udf_load_logicalvol function in fs/udf/super.c in the Linux kernel before 3.4.5 allows remote attackers to cause a denial of service (system crash) or possibly have unspecified other impact via a crafted UDF filesystem.

- **Question :** est-ce intéressant ?

Analyser un CVE noyau

- **CVE-2012-3510**

> Use-after-free vulnerability in the xacct_add_tsk function in kernel/tsacct.c in the Linux kernel before 2.6.19 allows local users to obtain potentially sensitive information from kernel memory or cause a denial of service (system crash) via a taskstats TASKSTATS_CMD_ATTR_PID command.

- **Question :** est-ce intéressant ?

Analyser un CVE noyau

- **CVE-2013-0217**

> Memory leak in drivers/net/xen-netback/netback.c in the Xen netback functionality in the Linux kernel before 3.7.8 allows guest OS users to cause a denial of service (memory consumption) by triggering certain error conditions.

- **Question :** est-ce intéressant ?

Analyser un CVE noyau

- **Conclusions sur les CVE**
  - Il y en a assez peu
  - Beaucoup sont inutiles
  - Bugs qui ont pignon sur rue : vite corrigés
  - Il est bon de **chercher d'autres bugs**

Chercher les bugs corrigés silencieusement

- **Les sources d'information**
  - Les mailing lists des développeurs
  - Le bug tracker RedHat (bugzilla)
  - OpenWall
  - Kerneloops.org
  - Le GIT kernel

Chercher les bugs corrigés silencieusement

- **Bugzilla**

> Description of the problem:
> Lack proper synchronization to manipulate inet->opt ip_options can lead to system crash.
> Problem is that ip_make_skb() calls ip_setup_cork() and ip_setup_cork() possibly makes a copy of ipc->opt (struct ip_options), without any protection against another thread manipulating inet->opt. Another thread can change inet->opt pointer and free old one under us.
> Given right server application (setting socket options and processing traffic over the same socket at the same time), remote attacker could use this flaw to crash the system. More likely though, local unprivileged user could use this flaw to crash the system.

Chercher les bugs corrigés silencieusement

- **[PATCH] ehea: Fix possible NULL pointer dereference**, *Syam Sidhardhan*
  - **Re: [PATCH] ehea: Fix possible NULL pointer dereference**, *Thadeu Lima de Souza Cascardo*
- **[PATCH] SUNRPC: Fix possible NULL pointer dereference**, *Syam Sidhardhan*
  - **Re: [PATCH] SUNRPC: Fix possible NULL pointer dereference**, *Myklebust, Trond*
    - **Re: [PATCH] SUNRPC: Fix possible NULL pointer dereference**, *Syam Sidhardhan*
- **[PATCH] rndis_wlan: Remove redundant NULL check before kfree**, *Syam Sidhardhan*
  - **Re: [PATCH] rndis_wlan: Remove redundant NULL check before kfree**, *Jussi Kivilinna*
- **Gianfar breaks one of my test configs**, *Benjamin Herrenschmidt*
  - **Re: Gianfar breaks one of my test configs**, *Paul Gortmaker*
  - **[PATCH net] gianfar: fix compile fail for NET_POLL=y due to struct packing**, *Paul Gortmaker*
    - **Re: [PATCH net] gianfar: fix compile fail for NET_POLL=y due to struct packing**, *David Miller*
- **[PATCH] xfrm_user: constify netlink dispatch table**, *Mathias Krause*
- **Problem with multicast traffic when using network bridging**, *Adam Baker*
- **Fw: [Bug 54281] New: kernel NULL pointer dereference on deleting a vlan interface**, *Stephen Hemminger*
  - **Re: Fw: [Bug 54281] New: kernel NULL pointer dereference on deleting a vlan interface**, *Cong Wang*
- **[PATCH 0/2] net: sock_diag fixes**, *Mathias Krause*
  - **[PATCH 1/2] sock_diag: Fix out-of-bounds access to sock_diag_handlers[]**, *Mathias Krause*
    - **Re: [PATCH 1/2] sock_diag: Fix out-of-bounds access to sock_diag_handlers[]**, *Eric Dumazet*
      - **Re: [PATCH 1/2] sock_diag: Fix out-of-bounds access to sock_diag_handlers[]**, *Mathias Krause*
  - **[PATCH 2/2] sock_diag: Simplify sock_diag_handlers[] handling in __sock_diag_rcv_msg**, *Mathias Krause*
  - **Re: [PATCH 0/2] net: sock_diag fixes**, *David Miller*
- **[PATCH] drivers/vhost: remove depends on CONFIG_EXPERIMENTAL**, *Kees Cook*
- **[PATCH] vxlan: remove depends on CONFIG_EXPERIMENTAL**, *Kees Cook*
  - **Re: [PATCH] vxlan: remove depends on CONFIG_EXPERIMENTAL**, *David Miller*
- **[PATCH] mlx4_en: fix allocation of CPU affinity reverse-map**, *Kleber Sacilotto de Souza*

Chercher les bugs corrigés silencieusement

Userland can send a netlink message requesting SOCK_DIAG_BY_FAMILY with a family greater or equal then AF_MAX -- the array size of sock_diag_handlers[]. The current code does not test for this condition therefore is vulnerable to an out-of-bound access opening doors for a privilege escalation.

```
---
diff --git a/net/core/sock_diag.c b/net/core/sock_diag.c
index 602cd63..750f44f 100644
--- a/net/core/sock_diag.c
+++ b/net/core/sock_diag.c
@@ -121,6 +121,9 @@ static int __sock_diag_rcv_msg(struct sk_buff *skb, struct
nlmsghdr *nlh)
        if (nlmsg_len(nlh) < sizeof(*req))
                return -EINVAL;

+       if (req->sdiag_family >= AF_MAX)
+               return -EINVAL;
+
        hndl = sock_diag_lock_handler(req->sdiag_family);
--
1.7.10.4
```

Chercher les bugs corrigés silencieusement

- **Les mailing lists développeurs**
  - Quantité énorme d'informations
  - Difficile à trier
  - Avantage : **on a les bugs avant qu'ils ne soient corrigés**

Le GIT

- **Le GIT noyau**
  - Intérêt : on voit toutes les modifications
  - Chaque commit contient un texte d'explication
  - L'output est facile à parser
  - On y trouve **tous les bugs patchés silencieusement**

Le GIT

commit a5cd335165e31db9dbab636fd29895d41da55dd2
Author: Xi Wang <xi.wang@gmail.com>
Date: Wed Nov 23 01:12:01 2011 -0500

drm: integer overflow in drm_mode_dirtyfb_ioctl()

There is a potential integer overflow in drm_mode_dirtyfb_ioctl() if userspace passes in a large num_clips. The call to kmalloc would allocate a small buffer, and the call to fb->funcs->dirty may result in a memory corruption.

Reported-by: Haogang Chen <haogangchen@gmail.com>

Le GIT

- **Le GIT : une mine d'or**
  - Les bugs corrigés silencieusement sont beaucoup plus intéressants
  - Problème : beaucoup trop d'informations
  - Solution : industrialiser le parsing

Le GIT

- **Industrialisation de la veille**
  - Analyse constante des commits noyaux
  - Recherche des patterns intéressants
  - Mise en valeur des éléments importants du commit
  - Interface permettant une sélection plus fine
  - Résultat : une veille constante, efficace et complète
- **Aller à l'essentiel**
  - Objectif : devenir root
  - Trier en fonction de la région du noyau touchée
  - Ecarter rapidement les bugs inutiles
  - Bien connaître sa cible
  - Approfondir l'étude d'un bug

- **Grandes étapes de l'étude d'un bug**
  - Trouver l'emplacement du bug dans les sources
  - Trouver un chemin d'accès vers la fonction vulnérable
  - Faire un PoC nous permettant de déclencher le bug
  - Coder l'exploit

- **Des outils utiles pour parcourir les sources**
  - Linux Cross Reference (LXR). Lxr.linux.no
  - Understand de SciTool
  - Cscope
- **Outils incontournables de debug noyau**
  - SystemTap
  - Vmware + GDB
  - Cscope

Questions ?

- **Etienne Comet / e.comet@lexfo.fr pour toutes questions sur la présentation**