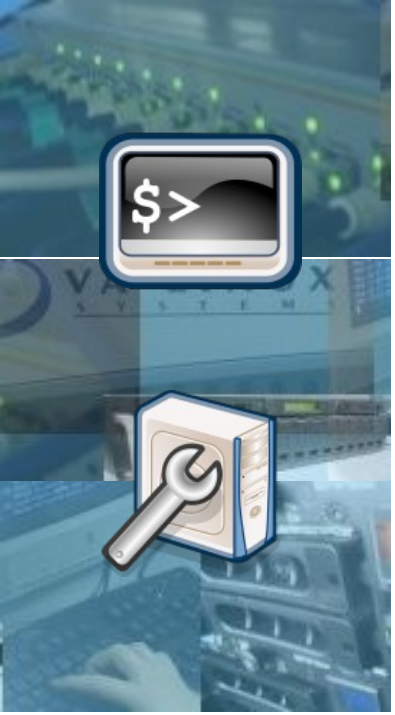


Sécurité et Open Source

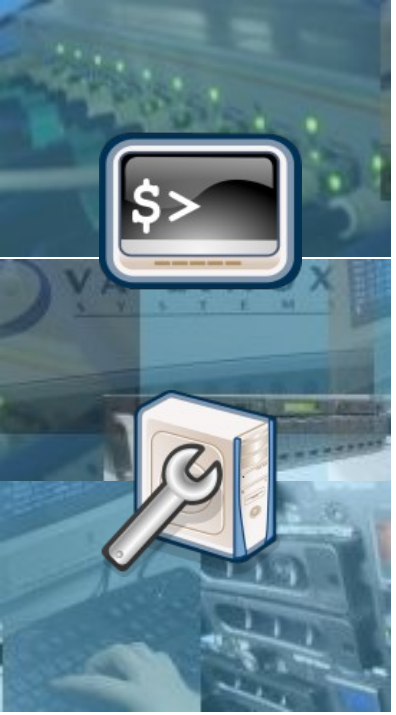
Synergie NTIC 2008 - Sécurité & Open Source

Grégory Colpart – Evolix / Debian

<reg@evolix.fr>

<reg@debian.org>

evolix
Informatique et Logiciels Libres

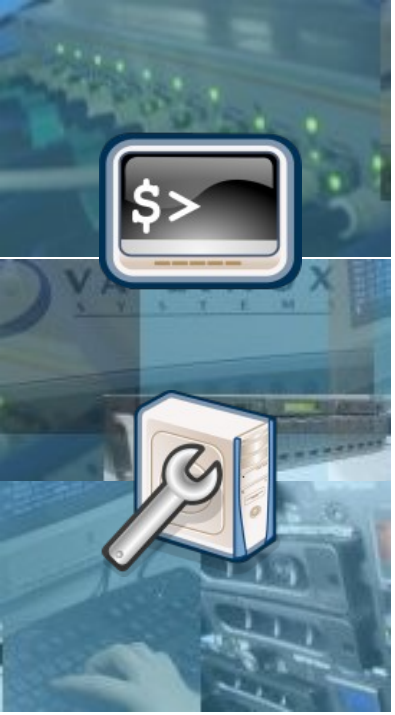


Synergie NTIC 2008 - Sécurité & Open Source

Plan

- Full Disclosure : mythe ou réalité ?
- Suivre la sécurité des systèmes et applications Open Source
- Applications OpenSource : vanilla sources ou packages ?
- Exemples concrets (Linux vmsplice local root exploit, Debian/openssl générateur de nombres aléatoires prévisibles Debian).

evolix
Informatique et Logiciels Libres

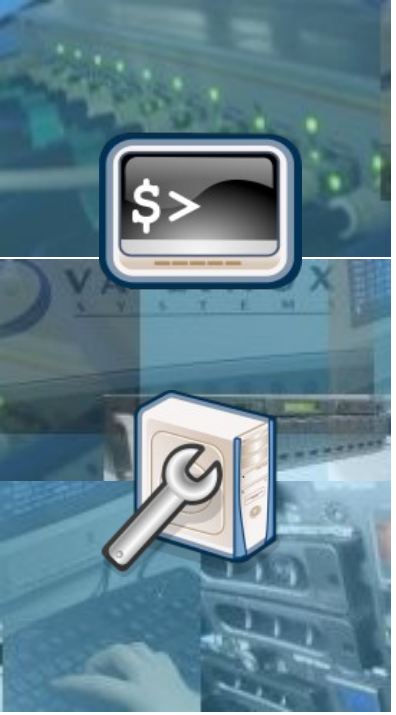


Synergie NTIC 2008 - Sécurité & Open Source

Vocabulaire

- Author/upstream
- Vendor
- BlackHat
- WhiteHat
- Script Kiddies
- Fix, Workaround
- Disclosure, Vulnerability
- Security Advisory

evolix
Informatique et Logiciels Libres



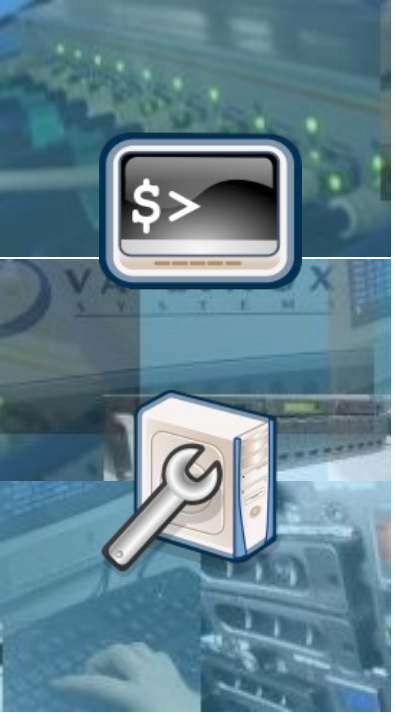
Synergie NTIC 2008 - Sécurité & Open Source

Full Disclosure

Le principe du Full Disclosure est de communiquer immédiatement et publiquement tous les détails concernant les problèmes de sécurité, notamment comment détecter et exploiter le problème. Ce principe a été créé pour **forcer** *upstreams* et *vendors* à corriger très vite le problème.

Par définition, un logiciel Open Source utilise plutôt ce principe.

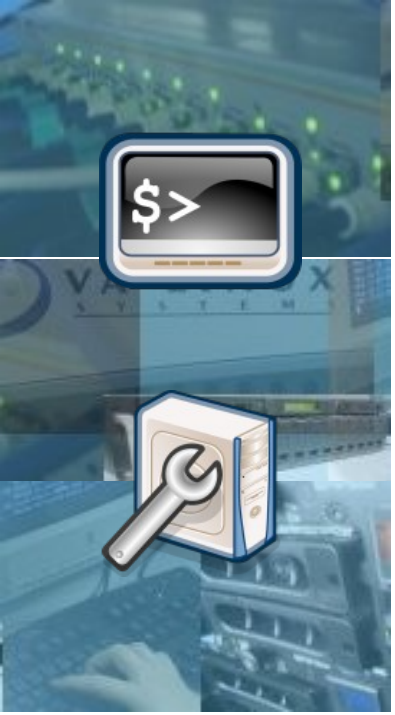
evolix
Informatique et Logiciels Libres



Security by Obscurity

À l'inverse, lorsque les informations à propos des problèmes de sécurités ne sont pas rendues publiques, et les alertes des BlackHat/WhiteHat sont « délayées » voire ignorées.

Les logiciels propriétaires ont tendance à utiliser ce principe.

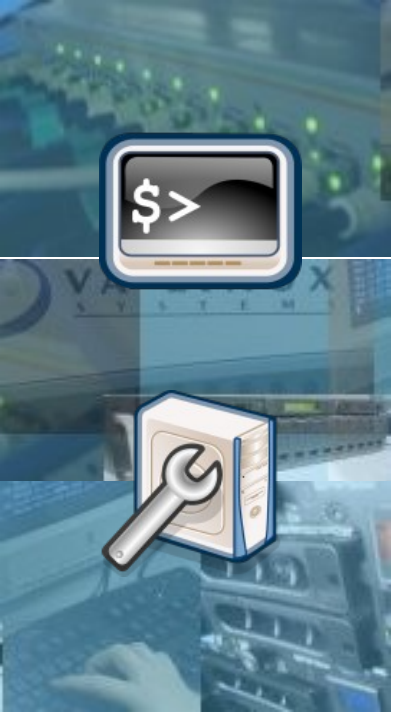


Synergie NTIC 2008 - Sécurité & Open Source

mais...

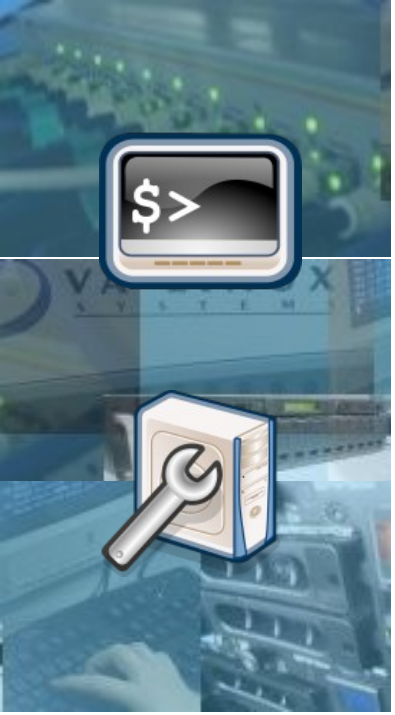
...le principe de "Full Disclosure" n'est pas aussi simple !

evolix
Informatique et Logiciels Libres



Problèmes upstream

Les problèmes détectés par les upstreams sont corrigés... selon le bon vouloir et le sérieux des auteurs. Pas grand chose à souligner là-dessus.

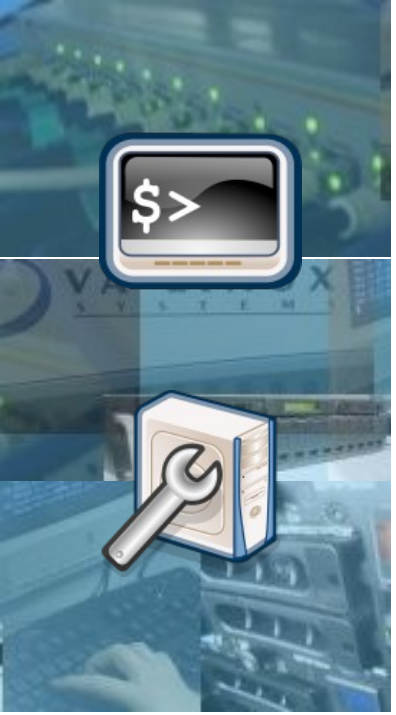


Synergie NTIC
2008 - Sécurité
& Open Source

Problèmes détectés par d'autres personnes

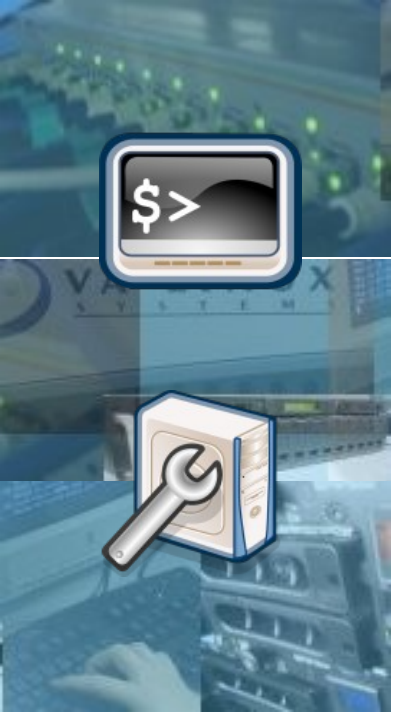
- Private Disclosure : gardées secrètement... et même vendues.
- Exploit 0-day : déclarés sans "sommation"
- Responsible/Limited Disclosure

evolix
Informatique et Logiciels Libres



Responsible Disclosure

Période de *Private Disclosure* pour permettre aux *upstreams* ou *vendors* de fixer le problème ou de sortir un *workaround*.
Cette période d'embargo est limitée (sorte d'ultimatum). Souvent, il s'agit de 14 jours... ou beaucoup moins pour certains logiciels/systèmes très critiques. La personne qui a découvert le problème (WhiteHat) est alors citée par l'upstream.
C'est en pratique la voie la plus classique pour tous les problèmes de sécurité sérieux avec l'Open Source.



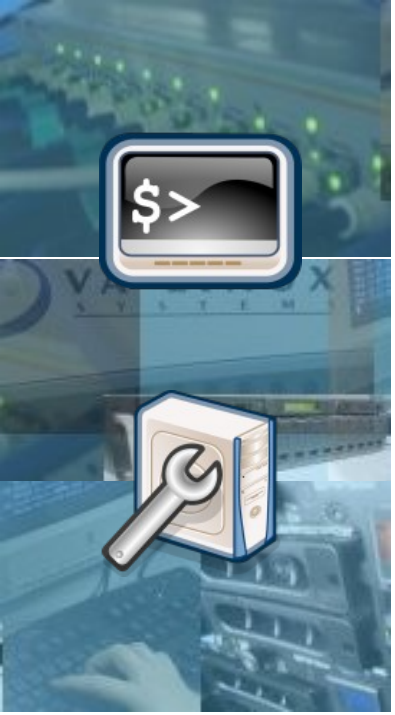
Synergie NTIC 2008 - Sécurité & Open Source

Problèmes pas encore détectés

... au boulot ! ;-)

Les audits de sécurité dans les logiciels Open Source dépendent ... du sérieux des upstreams, des vendors et des utilisateurs. C'est donc très variable d'un projet à l'autre. Il faut connaître l'organisation du développement et la communauté pour être capable de se prononcer sur la sécurité d'un logiciel Open Source.

evolix
Informatique et Logiciels Libres



Synergie NTIC 2008 - Sécurité & Open Source

Suivre la sécurité des systèmes/application Open Source

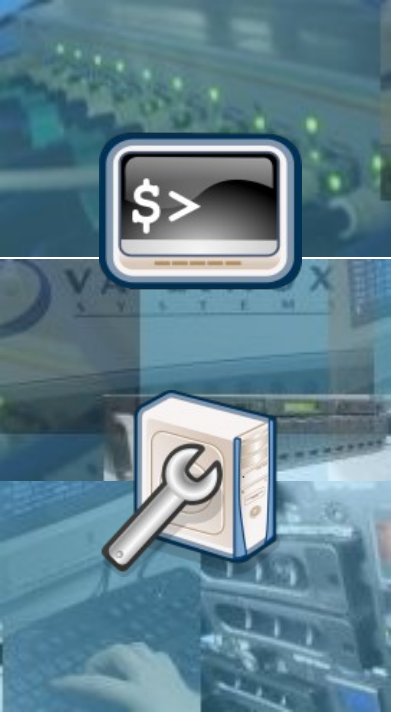
Listes de diffusion :

- Bugtraq
- Full-disclosure
- oss-security

System Advisories :

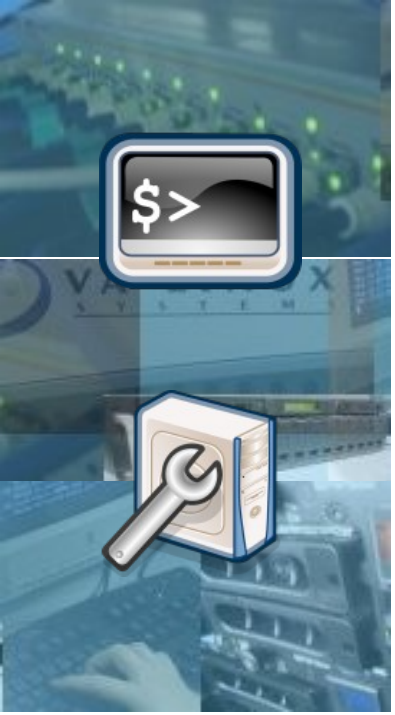
DSA, MDKSA, GLSA, USN, OpenBSD erratas, etc.

evolix
Informatique et Logiciels Libres



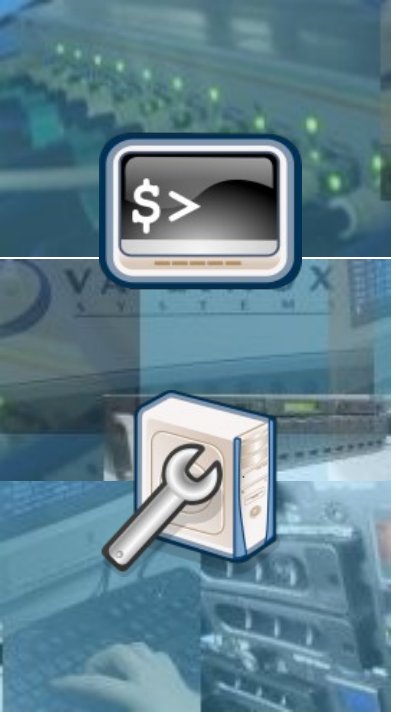
Informations spécifiques aux logiciels. Quelques exemples :
- phpMyAdmin -> PMASA
- Horde -> liste privée horde-vendor
- Flux RSS, *changelogs*, suivi des *commits*

Coordinations entre distributions :
CVE-ID (Common Vulnerabilities and Exposures ID)
Voir http://cve.mitre.org/



Exemple avec Debian

- Équipe Sécurité pour Stable
- Équipe Sécurité pour Testing avec un tracker http://security-tracker.debian.net/
- Bugs Debian tagués "security"
- IRC, alias security@/team@, etc.
- Upload public et privé



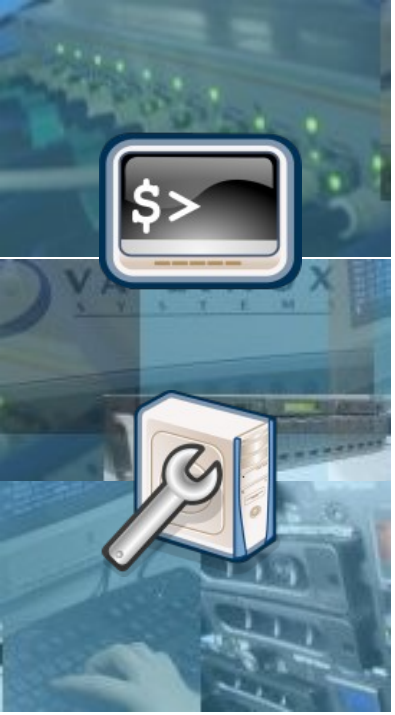
Vanilla sources VS packages

Avantages des vanilla sources

Maîtrise complète de la version :
- Choix de la version
- Possibilité d'avoir une version up-to-date.
- Compilation spécifique

Avantages des packages/ports

- Installation/mise-à-jour aisées.
- Problèmes de sécurité sensés être suivis, a priori pas besoin d'une veille/suivi sécurité trop intense.



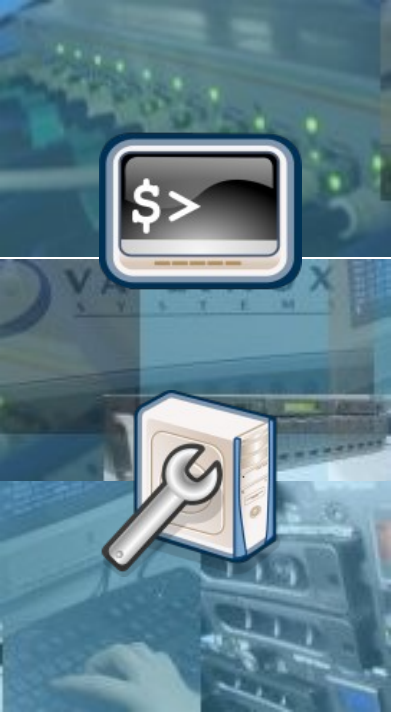
Synergie NTIC 2008 - Sécurité & Open Source

Conlusion : dans le cas d'une utilisation d'une distribution communautaire (Debian, Fedora, etc.), participer à la veille/suivi sécurité

Exemples de choix sources VS packages :

- noyau Linux
- Apache, MySQL, PostgreSQL, etc.
- PHP, Java, etc.
- web-apps : CMS, webmail, etc.

evolix
Informatique et Logiciels Libres



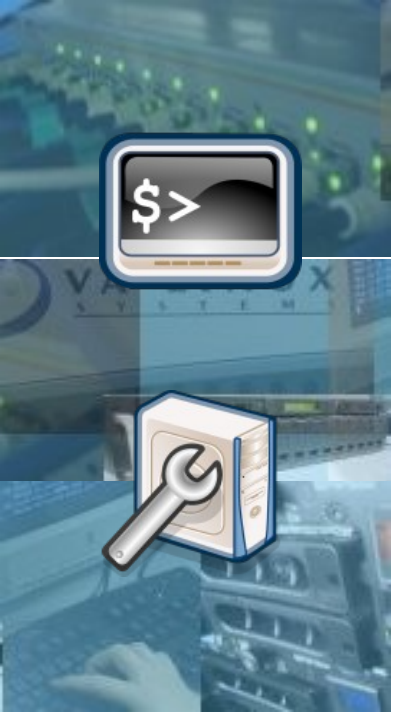
Synergie NTIC
2008 - Sécurité
& Open Source

Exemples concrets

Linux vmsplice local root exploit

Correctifs 2.6.24.1 et 2.6.24.2

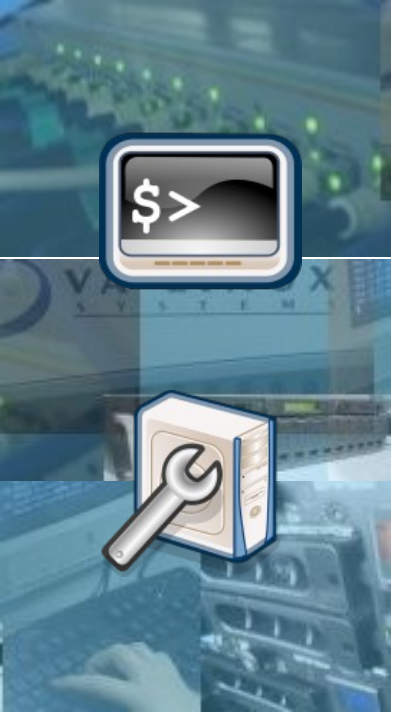
evolix
Informatique et Logiciels Libres



Synergie NTIC 2008 - Sécurité & Open Source

16:19 -!- waldi [~waldi@bblank.thinkmo.de] has joined #debian-security
17:13 < aba> anyone of you reviewed
http://134.2.34.20/blank/debian/linux-2.6/ already?
17:15 < waldi> http://194.39.182.225/debian/linux-2.6/security.patch
...
18:55 < fw> waldi: The vserver-/proc issue is CVE-2008-0163.
18:55 < waldi> too late, will note it later in the changelog
...
19:29 < waldi> there are two possibilities now: upload to stable-security or dump it
19:42 < sf> fw: ^
19:42 < sf> does the vserver issue affect only etch or also lenny and sid?
19:49 < waldi> only etch
19:51 < sf> ok, thanks
19:53 < waldi> anyway, the kernel team does the security releases on its own. usualy handled by dannf. who wants to play proxy?
20:00 -!- waldi [~waldi@bblank.thinkmo.de] has left #debian-security []

evolix
Informatique et Logiciels Libres

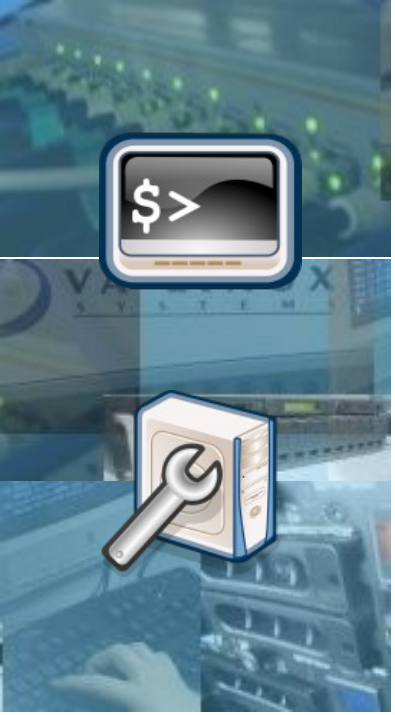


Synergie NTIC 2008 - Sécurité & Open Source

http://kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.24.2
commit 1617e66d11d6621824f642728d62f242272fd063
Author: Bastian Blank <bastian@waldi.eu.org>
Date: Sun Feb 10 16:47:57 2008 +0200

http://lists.debian.org/debian-security-announce/2008/msg00056.html
Subject: [SECURITY] [DSA 1494-1] New linux-2.6 packages fix privilege escalation
Date: Mon, 11 Feb 2008 14:58:39 +0100

evolix
Informatique et Logiciels Libres

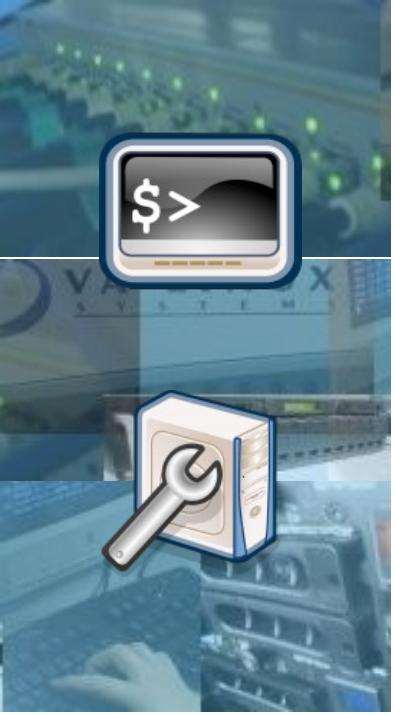


Synergie NTIC 2008 - Sécurité & Open Source

Générateur de nombres aléatoires prévisibles avec le package Debian openssl

BTS http://bugs.debian.org/363516

evolix
Informatique et Logiciels Libres

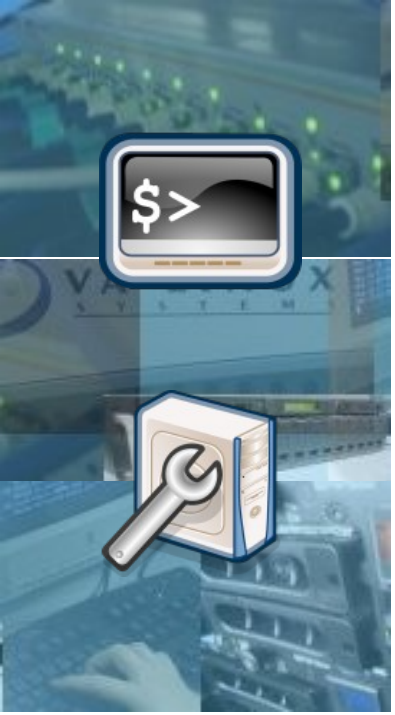


Synergie NTIC 2008 - Sécurité & Open Source

Date: Thu, 4 May 2006 20:40:03 +0200
Source: openssl
Binary: libssl-dev openssl libssl0.9.8-dbg libcrypto0.9.8-udeb libssl0.9.8
Architecture: source i386
Version: 0.9.8b-1
Distribution: unstable

* Don't add uninitialised data to the random number generator. This stop valgrind from giving error messages in unrelated code. (Closes: #363516)

evolix
Informatique et Logiciels Libres



Synergie NTIC 2008 - Sécurité & Open Source

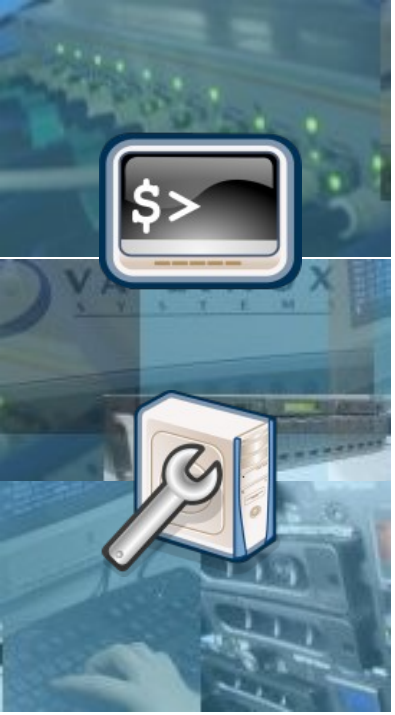
http://svn.debian.org/viewsvn/pkg-openssl/openssl/trunk/crypto/rand/md_rand.c?rev=300&r1=199&r2=300

```
*** openssl/trunk/crypto/rand/md_rand.c 2007/02/23 19:43:27 199
--- openssl/trunk/crypto/rand/md_rand.c 2008/05/07 18:35:39 300
***************
*** 271,280 ****
        else
            MD_Update(&m,&(state[st_idx]),j);

- /*
-  * Don't add uninitialised data.
        MD_Update(&m,buf,j);
- */
        MD_Update(&m,(unsigned char *)&(md_c[0]),sizeof(md_c));
        MD_Final(&m,local_md);
        md_c[1]++;
--- 271,277 ----
```

evolix

Informatique et Logiciels Libres

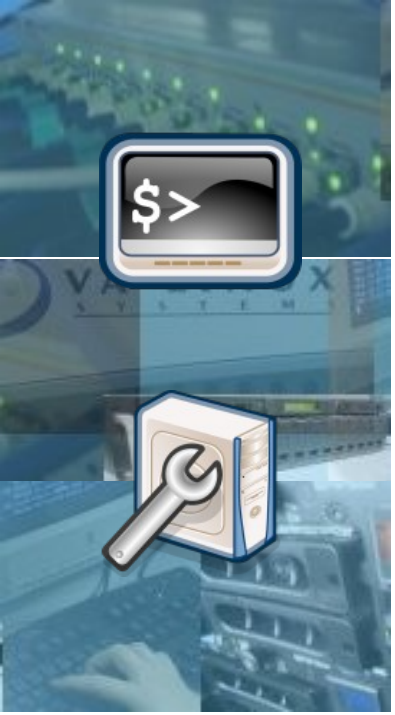


Synergie NTIC 2008 - Sécurité & Open Source

http://lists.debian.org/debian-security-announce/2008/msg00152.html
Subject: [SECURITY] [DSA 1571-1] New openssl packages fix predictable random number generator
Date: Tue, 13 May 2008 14:06:39 +0200

openssh-blacklist (0.1.0) unstable; urgency=low
  * Upload to unstable.
 -- Colin Watson <cjwatson@debian.org> Tue, 13 May 2008 14:55:25 +0100
openssh-blacklist (0.1) stable-security; urgency=low
  * Initial release.
 -- Kees Cook <kees@outflux.net> Fri, 09 May 2008 15:44:32 -0700

evolix
Informatique et Logiciels Libres



Synergie NTIC 2008 - Sécurité & Open Source

« That's all folks! »

Grégory Colpart – Evolix / Debian

<reg@evolix.fr>

<reg@debian.org>

evolix

Informatique et Logiciels Libres