FreeBSD VuXML

Renato Botelho <garga@FreeBSD.org>

05 de Dezembro de 2009

BluePex Security Solutions
The FreeBSD Project

BluePex™ SECURITY SOLUTIONS

Agenda

- FreeBSD
- FreeBSD ports collection
- VuXML
- FreeBSD VuXML
- vxquery
- portaudit

FreeBSD

- SO derivado do UNIX BSD (1978, 1992)
- Completo: kernel + user space
- Licença BSD
- Foco em reuso comercial
- Documentação
- Security Officer
- Ports collection

Ports collection

- Quase 21.000 aplicativos disponíveis
- Divididos em subcategorias
- Pacotes binários
- Ferramentas para atualização
  - portmaster
  - portupgrade
  - portmanager

VuXML

- Criado em 2005 por Jacques A. Vidrine
- Formato de documento para descrever vulnerabilidades
- Não é um banco de dados
- Uma aplicação XML
- VuXML.org website
- Aplicativos
  - portaudit
  - vxquery

Objetivos

- Descever as vulnerabilidades
- Precisão nas versões
- Geração de conteúdo de fácil leitura
- Colaboração
- Editável “na unha”
- Integrado com o freshports.org
- Fácil adaptação a qualquer sistema

VuXML no FreeBSD

- Adotado em 2005
- 1360 vulnerabilidades cadastradas
- 2075 commits
- 92 committers
- 250 colaboradores

Quem é responsável?

- FreeBSD Security Team
- Qualquer committer pode modificar
- Colaborações podem ser enviadas através do send-pr ou em http://bugs.FreeBSD.org

Criando nova entrada

```
# cd /usr/ports/security/vuxml
# make install clean

Serão instalados todos os softwares
necessários mais o DTD, modelos e
catálogos.

# make newentry

Uma nova entrada é criada, com um ID
único, gerado com o uuidgen(1)

# make validate
```

```
<vuln vid="5cb2ad6a-e028-11de-8c29-001d0fbf2026">
  <topic> -- </topic>
  <affects>
    <package>
 <name></name>
 <range><lt></lt></range>
    </package>
  </affects>
  <description>
    <body xmlns="http://www.w3.org/1999/xhtml">
 <p>SO-AND-SO reports:</p>
 <blockquote cite="INSERT URL HERE">
   <p>.</p>
 </blockquote>
    </body>
  </description>
  <references>
  </references>
  <dates>
    <discovery>2009-12-FIXME</discovery>
    <entry>2009-12-03</entry>
  </dates>
</vuln>
```

Exemplo de entrada

```
<vuln vid="77c14729-dc5e-11de-92ae-02e0184b8d35">
 <topic>libtool -- Library Search Path Privilege
Escalation Issue</topic>
 <affects>
  <package>
   <name>libtool</name>
   <range><lt>2.2.6b</lt></range>
  </package>
 </affects>
 <description>
  <body xmlns="http://www.w3.org/1999/xhtml">
   <p>Secunia.com</p>
   <blockquote
cite="http://secunia.com/advisories/37414/">
    <p>Do not attempt to load an unqualified module.la
       file from the current directory (by default)
       since doing so is insecure and is not compliant
       with the documentation.</p>
```

Exemplo de entrada (cont)

```
   </blockquote>
  </body>
 </description>
 <references>
  <url>http://secunia.com/advisories/37414/</url>
  <url>http://lists.gnu.org/archive/html/libtool/2009-
11/msg00059.html</url>
 </references>
 <dates>
  <discovery>2009-11-25</discovery>
  <entry>2009-11-28</entry>
 </dates>
</vuln>
```

vxquery

```
Topic: Apache 1.3 IP address access control failure on
some 64-bit platforms
Affects:
   apache < 1.3.29_2
   apache+mod_ssl < 1.3.29+2.8.16_1
   apache+ssl < 1.3.29.1.53_1
   ru-apache < 1.3.29+30.19_1
   ru-apache+mod_ssl < 1.3.29+30.19+2.8.16_1
References:
   cvename:CVE-2003-0993
   url:http://cvs.apache.org/viewcvs.cgi/...
   url:http://www.apacheweek.com/features/security-13
   url:http://nagoya.apache.org/bugzilla/show_bug.cgi?
id=23850
   mlist:http://marc.theaimsgroup.com/?l=apache-
cvs&m=107869603013722
   bid:9829
<URL:http://vuxml.freebsd.org/09d418db-70fd-11d8-873f-
0020ed76ef5a.html>
```

portaudit

- Checar vulnerabilidades dos ports do FreeBSD no VuXML
- Prevenir instalação de ports vulneráveis
- Alertar sobre vulnerabilidades em ports já instalados
- Integrado automaticamente com o SO

Proteção na instalação

```
root@srv1:/usr/ports/graphics/php4-gd# make
===>  php4-gd-4.4.9 has known vulnerabilities:
=> gd -- '_gdGetColors' remote buffer overflow
vulnerability.
   Reference:
<http://portaudit.FreeBSD.org/4e8344a3-ca52-11de-
8ee8-00215c6a37bb.html>
=> Please update your ports tree and try again.
*** Error code 1

Stop in /usr/ports/graphics/php4-gd.
*** Error code 1

Stop in /usr/ports/graphics/php4-gd.
Exit 1
```

gd -- '_gdGetColors' remote buffer overflow vulnerability

Description:

CVE reports:

> The _gdGetColors function in gd_gd.c in PHP 5.2.11 and 5.3.0, and the GD Graphics Library 2.x, does not properly verify a certain colorsTotal structure member, which might allow remote attackers to conduct buffer overflow or buffer over-read attacks via a crafted GD file, a different vulnerability than CVE-2009-3293.

References:

- BugTraq ID 36712
- CVE name CVE-2009-3546
- URL: <http://secunia.com/advisories/37069>
- URL: <http://secunia.com/advisories/37080>

Affects:

- gd <2.0.35_2,1
- php5-gd <5.2.11_2
- php4-gd >0

Oliver Eikemeier <eik@FreeBSD.org>

Alerta sobre pacotes instalados

```
Downloading fresh database.
auditfile.tbz                          58 kB   47 kBps
New database installed.
Database created: Thu Dec  3 02:40:01 BRST 2009

Checking for packages with security
vulnerabilities:

Affected package: libtool-1.5.26
Type of problem: libtool -- Library Search Path
Privilege Escalation Issue.
Reference:
<http://www.FreeBSD.org/ports/portaudit/77c14729-
dc5e-11de-92ae-02e0184b8d35.html>
```

freshports.org

The FreshPorts Search

Port Name ▼ | containing ▼ | php4-gd | 10 results ▼

☐ Include deleted ports ☐ Case sensitive search Sort by: Category ▼ ascending ▼ Search

☐ Include /src tree

Notes

- Case sensitivity is ignored for "sounds like" and output is ordered by the soundex.
- When searching on 'Message ID', the type of match is ignored.
- When searching on 'Commit Message' only 'containing' is used.
- When searching by 'Under a pathname', your path must start with something like /ports/, /doc/, or /src/. All commits under that point will be returned. The selected match type is ignored and defaults to 'Starts with'.

Number of ports: 1

php4-gd 4.4.9 graphics

The gd shared extension for php

Maintained by: ale@Free

An older version of this port was marked as vulnerable.

CVSWeb : Sources : Main Web Site : Distfiles Availability : PortsMon

---

To install the port: `cd /usr/ports/graphics/php4-gd/ && make install clean`
To add the package: `pkg_add -r php4-gd`

Number of ports: 1

Dúvidas ?

Obrigado!