VuXML — Vulnerabilities and Exposures Markup Language

BSDCan 2005

Jacques Vidrine
<nectar@FreeBSD.org>

What is VuXML?

- a document format for describing security issues that affect a software collection
- NOT a database
- an XML application (so is XHTML, SVG, MathML, RDF, Docbook XML)

FreeBSD Ports Collection

- A collection of software packages– currently over 12,000
- The packages are built from the "ports tree"
- Each "port" is a collection of files that automate building, installation, and packaging the software
- Similar collections exist for other operating systems. Terminology varies.

Let's take a peek

```
<vuxml xmlns="http://www.vuxml.org/apps/vuxml-1">
  <vuln vid="1d3a2737-7eb7-11d9-acf7-000854d03344">
    <topic>unace -- multiple vulnerabilities</topic>
    <affects>
      <package>
        <name>unace</name>
        <range><lt>unace-1.2b_2</lt></range>
      </package>
    </affects>
    <description>
      <body xmlns="http://www.w3.org/1999/xhtml">
        <p>Ulf Härnhammar reports multiple security vulnerabilities in unace-1.2b:</p>
        <ul>
          <li>There are buffer overflows when extracting, testing or listing specially prepared
            ACE archives.</li>
          <li>There are directory traversal bugs when extracting ACE archives.</li>
          <li>There are also buffer overflows when dealing with long (>17000 characters) command
            line arguments.</li>
        </ul>
      </body>
    </description>
    <references>
      <cvename>CAN-2005-0160</cvename>
      <cvename>CAN-2005-0161</cvename>
    </references>
    <dates>
      <discovery>2005-02-14</discovery>
      <entry>2005-02-22</entry>
    </dates>
  </vuln>
```

Let's take a peek

unace -- multiple vulnerabilities

FreeBSD VuXML: Documenting security issues in FreeBSD and the FreeBSD Ports Collection

Affected packages
unace < unace-1.2b_2

Details

VuXML ID	1d3a2737-7eb7-11d9-acf7-000854d03344
Discovery	2005-02-14
Entry	2005-02-22

Ulf Härnhammar reports multiple security vulnerabilities in unace-1.2b:

- There are buffer overflows when extracting, testing or listing specially prepared ACE archives.
- There are directory traversal bugs when extracting ACE archives.
- There are also buffer overflows when dealing with long (>17000 characters) command line arguments.

References

CVE Name	CAN-2005-0160
CVE Name	CAN-2005-0161

VuXML is also...

- VuXML.org web sites
- Tools for processing VuXML
  - portaudit, vxquery
- VuXML document instances
  - the FreeBSD VuXML Document
  - the OpenBSD VuXML Document

Why was VuXML created?

- FreeBSD Security Officer charter says
  - "The FreeBSD Security Officer's mission is to protect the FreeBSD user community by keeping the community informed of bugs, exploits, popular attacks, and other risks; [...]"
- Security Advisories, Security Notices too heavy for frequent updates

Some goals

- Rich descriptions
- Precise version information
- Sanity checking
- Easily generated human readable output
- Collaborative
- Editable "by hand"

Other approaches

Web application

- Adopt NetBSD pkg-vulnerabilities (package, type, URL) or something like it
- CVE, Open Vulnerabilities and Assessment Language (OVAL)

Some XML advantages

- Encoding, parsing well-defined
- Leverage XHTML for narrative descriptions of security issues
- Validation
- XPath allows structure to evolve
- XSLT makes presentation easy

VuXML today

- Over 1 year old: February 2004
- Projects documenting issues with VuXML: FreeBSD, OpenBSD
  - FreeBSD VuXML document in ports CVS
  - vxquery, portaudit
  - VuXML.org, syndication
  - FreshPorts.org

FreeBSD VuXML document

/usr/ports/security/vuxml> - nectar@madman (0)

```
----------------------------
revision 1.281
date: 2004/10/12 00:57:22;  author: nectar;  state: Exp;  lines: +135 -15
Update the description of and list of packages affected by the PHP file
upload processing bug.

Submitted by:   Jon Passki <cykyc@yahoo.com>
----------------------------
revision 1.280
date: 2004/10/08 16:50:15;  author: nectar;  state: Exp;  lines: +32 -1
Document unsafe use of environmental variable SASL_PATH in cyrus-sasl.
----------------------------
revision 1.279
date: 2004/10/05 19:28:26;  author: trhodes;  state: Exp;  lines: +15 -3
Add some more apache ports.
Fix two errors found by nectar.
,log
    </description>
    <references>
      <url>http://www.hornik.sk/SA/SA-20040802.txt</url>
      <url>http://secunia.com/advisories/12156</url>
    </references>
    <dates>
      <discovery>2004-08-02</discovery>
      <entry>2004-10-05</entry>
    </dates>
  </vuln>

  <vuln vid="562a3fdf-16d6-11d9-bc4a-000c41e2cdad">
    <topic>php -- vulnerability in RFC 1867 file upload
    <affects>
      <package>
        <name>php4</name>
        <name>php4-cgi</name>
vuln.xml----------------------------------------------0 0x0  885/,0-1 56%
```

/usr/ports/security/vuxml> - nectar@madman (0)

```
ports/security/vuxml> cvs update
cvs update: Updating .
P vuln.xml
cvs update: Updating files
ports/security/vuxml> make validate
>>> Validating...
/usr/local/bin/xmllint --valid --noout /usr/ports/security/vuxml/vuln.xml
>>> Successful.
ports/security/vuxml>
```

VuXML.org

OpenBSD VuXML – entry date index

http://www.vuxml.org/openbsd/

OpenBSD VuXML

Documenting security issues in the OpenBSD Ports & Packages Collection

Security issues that affect the OpenBSD Ports & Packages Collection
the **Vulnerabilities and Exposures Markup Language (*VuXML*)**
document that serves as the source for the content of this site can b
anonymous CVS tree at anoncvs@beastie.hu:/cvs, file vuxml/vuln.x

entry date index

by package name | by topic | by CVE name | by entry date | by mod

Entered	Topic
2005-05-05	leafnode -- denial of service
2005-05-01	ImageMagick -- ReadPNMImage() heap overflow vu
2005-04-27	p5-Convert-UUlib -- buffer overflow
2005-04-12	xv -- multiple buffer overflows
2005-04-11	rsnapshot -- local privilege escalation
2005-04-07	gaim -- multiple vulnerabilities
2005-04-04	php4 -- multiple vulnerabilities
	php5 -- multiple vulnerabilities
	sylpheed -- message reply buffer overflow vulnerab
2005-03-27	gnupg -- OpenPGP protocol attack
	tiff -- multiple vulnerabilities
2005-03-23	jabberd -- multiple vulnerabilities
2005-03-22	grip -- CDDB response multiple matches buffer overflow vulnerability

Done

FreeBSD VuXML – mozilla

http://www.vuxml.org/freebsd/pkg-mozilla.html

mozilla

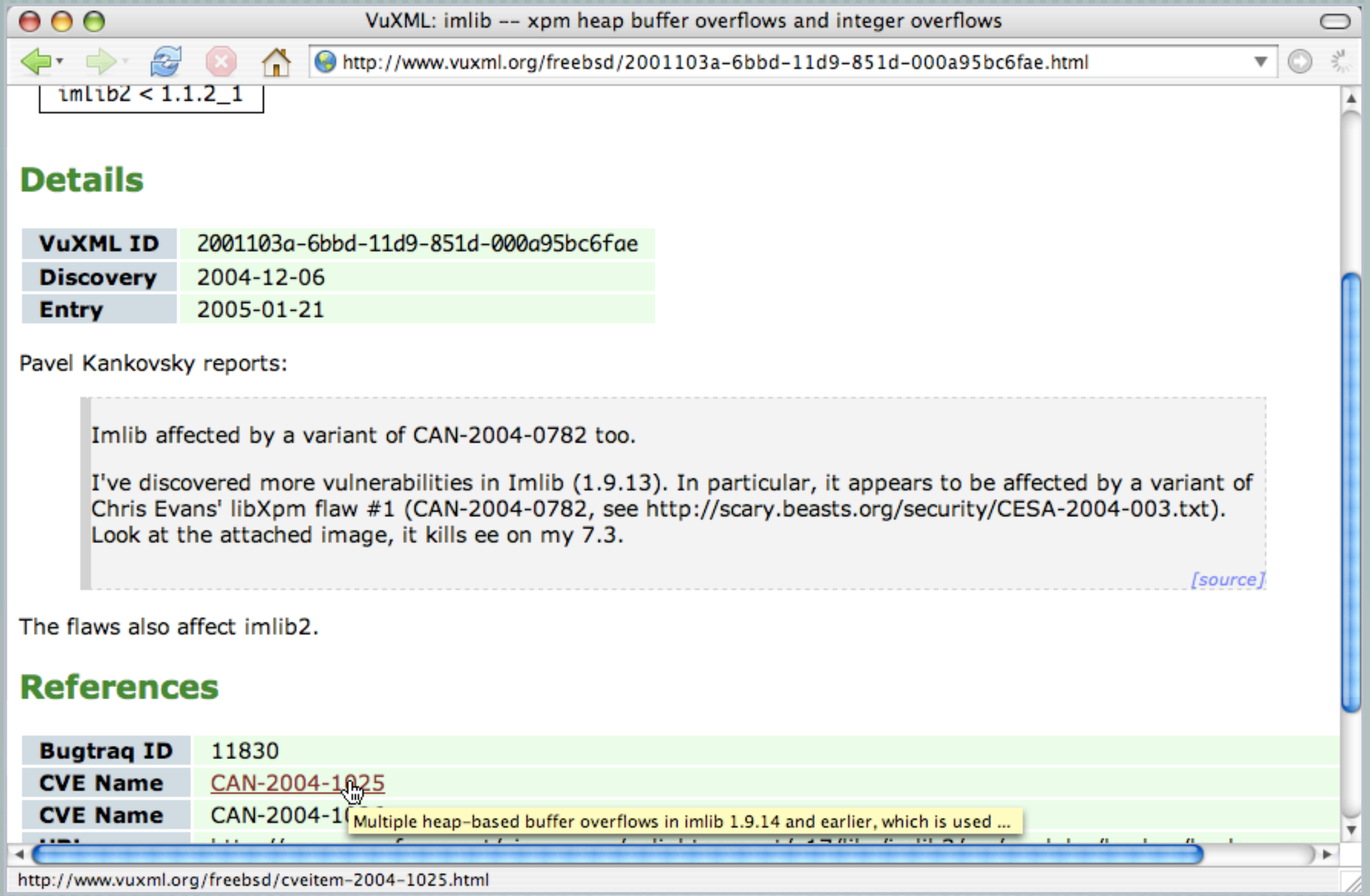
by package name | by topic | by CVE name | by entry date | by modified date | by VuXML ID

mozilla at FreshPorts.org

Entered	Topic
2005-04-16	mozilla -- javascript "lambda" replace exposes memory contents
	mozilla -- code execution through javascript: favicons
	mozilla -- privilege escalation via DOM property overrides
2005-03-24	mozilla -- heap buffer overflow in GIF image processing
2005-02-26	mozilla -- arbitrary code execution vulnerability
	mozilla -- insecure temporary directory vulnerability
2005-01-24	web browsers -- window injection vulnerabilities
2005-01-18	mozilla -- insecure permissions for some downloaded files
2005-01-13	mozilla -- heap overflow in NNTP handler
2004-09-30	mozilla -- hostname spoofing bug
	mozilla -- scripting vulnerabilities
	mozilla -- users may be lured into bypassing security dialogs
2004-09-28	mozilla -- BMP decoder vulnerabilities
	mozilla -- multiple heap buffer overflows
	mozilla -- vCard stack buffer overflow
2004-09-22	mozilla -- automated file upload
	mozilla -- built-in CA certificates may be overridden
	mozilla -- NULL bytes in FTP URLs
	mozilla -- security icon spoofing

Done

VuXML.org


VuXML: imlib -- xpm heap buffer overflows and integer overflows
http://www.vuxml.org/freebsd/2001103a-6bbd-11d9-851d-000a95bc6fae.html
imlib2 < 1.1.2_1
Details
VuXML ID 2001103a-6bbd-11d9-851d-000a95bc6fae
Discovery 2004-12-06
Entry 2005-01-21
Pavel Kankovsky reports:
Imlib affected by a variant of CAN-2004-0782 too.
I've discovered more vulnerabilities in Imlib (1.9.13). In particular, it appears to be affected by a variant of Chris Evans' libXpm flaw #1 (CAN-2004-0782, see http://scary.beasts.org/security/CESA-2004-003.txt). Look at the attached image, it kills ee on my 7.3.
[source]
The flaws also affect imlib2.
References
Bugtraq ID 11830
CVE Name CAN-2004-1025
CVE Name CAN-2004-1
Multiple heap-based buffer overflows in imlib 1.9.14 and earlier, which is used ...
http://www.vuxml.org/freebsd/cveitem-2004-1025.html

VuXML.org

VuXML: CAN-2005-0704

http://www.vuxml.org/freebsd/cveitem-2005-0704.html

CAN-2005-0704

FreeBSD VuXML: Documenting security issues in FreeBSD and the FreeBSD Ports Collection

This CVE name corresponds to:

Entered	Topic
2005-03-14	ethereal -- multiple protocol dissectors vulnerabilities

The following information is adapted from the Common Vulnerabilities and Exposures (CVE) project. CVE and the CVE logo are trademarks of The MITRE Corporation. CVE content is Copyright 2005, The MITRE Corporation.

CAN-2005-0704 at cve.mitre.org

Details

Type	Candidate
Name	CAN-2005-0704
Phase	Assigned*(20050309)*

Description

Buffer overflow in the Etheric dissector in Ethereal 0.10.7 through 0.10.9 allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code.

References

Source	Reference
CONFIRM	http://www.ethereal.com/appnotes/enpa-sa-00018.html
GENTOO	GLSA-200503-16
MANDRAKE	MDKSA-2005:053

http://www.gentoo.org/security/en/glsa/glsa-200503-16.xml

FreshPorts.org

FreshPorts -- net/gaim

http://www.freshports.org/net/gaim

Commit History - (may be incomplete: see CVSWeb link a

Date	By	Description
06 Apr 2005 03:46:39 **1.2.1**	marcus	Update to 1.2.1. See http: changes. Submitted by: Matthew Luc Security: See http:/ resolved i
03 Apr 2005 19:18:04 **1.2.0_2**	marcus	Disable GnuTLS support by by NSS. o requested by: pav
03 Apr 2005 07:36:11 **1.2.0_1**	marcus	* Add Perl option (disable * Unconditionally enable/di * TCL_VER: - is now TCLTK_VER Tk support) - has no effect un - is not mandatory * Minor cleanups (s/--enabl PR: 79157 Submitted by: Jean-Yves
20 Mar 2005 18:31:11 **1.2.0**	marcus	Fix the build on 4.X. Submitted by: Roman Shte
20 Mar 2005 03:52:00 **1.2.0**	marcus	Update to 1.2.0. ChangeLo http://gaim.sourceforge.net
12 Mar 2005 09:59:39 **1.1.4_1**	marcus	Chase the evolution-data-s

This port version is marked as vulnerable.

http://www.freshports.org/vuxml.php?vid=ec09baa3-a9f5-11d9-a788-0001(

Mozilla Firefox

http://www.freshports.org/vuxml.php?vid=ec09b

FreshPorts - VuXML

This page displays vulnerability information about FreeBSD Ports.

The last vuln.xml file processed by FreshPorts is:

```
Revision:  1.652
Date:      2005/05/03
Time:      10:14:18
Committer: sem
```

List all Vulnerabilities

These are the vulnerabilities relating to the commit you have selected:

VuXML ID	Description
ec09baa3-a9f5-11d9-a788-0001020eed82	gaim -- remote DoS on receiving certain messages over IRC The GAIM team reports: The IRC protocol plugin in Gaim 1.2.0, and possibly earlier versions, allows (1) remote attackers to inject arbitrary Gaim markup via irc_msg_kick, irc_msg_mode, irc_msg_part, irc_msg_quit, (2) remote

Done

vxquery

```
~> - nectar@madman (1)
~> vxquery
VuXML Query Tool (vxquery) 0.2
Report bugs to nectar@celabo.org

Usage:   vxquery [options] {filename} {package1} {package2} ... {packageN}
Options:
  -a          Output *all* entries.
  -d {dir}    Write output files into specified directory.
  -f {file}   Read package names from specified file.
  -h          Display this usage summary.
  -t {format} Choose output format.
Formats: text, vuxml, xhtml, xhtml-files
~>
```

```
/usr/ports/security/vuxml> - nectar@madman (1)
adPNMImage() heap overflow vulnerability

imsgroup.com/?l=bugtraq&m=111445767107869
<URL:http://vuxml.freebsd.org/cd286cc5-b762-11d9-bfb7-000c6ec775d9.html>

Topic: mplayer & libxine -- MMS and Real RTSP buffer overflow vulnerabilities
Affects:
    mplayer < 0.99.7
    mplayer-gtk < 0.99.7
    mplayer-gtk2 < 0.99.7
    mplayer-esound < 0.99.7
    mplayer-gtk-esound < 0.99.7
    mplayer-gtk2-esound < 0.99.7
    0.9.9 <= libxine < 1.0.1
References:
    bid:13270
    bid:13271
    cvename:CAN-2005-1195
    url:http://www.mplayerhq.hu/homepage/design7/news.html#vuln10
    url:http://www.mplayerhq.hu/homepage/design7/news.html#vuln11
    url:http://xinehq.de/index.php/security/XSA-2004-8
<URL:http://vuxml.freebsd.org/91c606fc-b5d0-11d9-a788-0001020eed82.html>

Topic: kdelibs -- kimgio input validation errors
byte 921
```

```
References

Bugtraq ID 13270
Bugtraq ID 13271
CVE Name   CAN-2005-1195
URL        http://www.mplayerhq.hu/homepage/design7/news.ht
URL        http://www.mplayerhq.hu/homepage/design7/news.ht
URL        http://xinehq.de/index.php/security/XSA-2004-8

kdelibs -- kimgio input validation errors

Affects

3.2 <= kdelibs < 3.4.0_2

Description

A KDE Security Advisory reports:

    kimgio contains a PCX image file format reader that doe
    perform input validation. A source code audit performed
    team discovered several vulnerabilities in the PCX and
    format readers, some of them exploitable to execute arb
<=UpDn Viewing <vxquery report>
```

portaudit

```
i:Exit  -:PrevPg  <Space>:NextPg v:View Attachm.  d:Del

Checking setuid files and devices:

Checking for uids of 0:
root 0
toor 0

Checking for passwordless accounts:

madman.celabo.org login failures:

madman.celabo.org refused connections:

Checking for a current audit database:

Database created: Fri May  6 02:40:08 CDT 2005

Checking for packages with security vulnerabilities:

Affected package: ImageMagick-6.2.0.5
Type of problem: ImageMagick -- ReadPNMImage() heap overf
vulnerability.
Reference:
<http://www.FreeBSD.org/ports/portaudit/cd286cc5-b762-11c

Affected package: mplayer-gtk-esound-0.99.6_1
Type of problem: mplayer & libxine -- MMS and Real RTSP buffer overflow
vulnerabilities.
Reference:
<http://www.FreeBSD.org/ports/portaudit/91c606fc-b5d0-11d9-a788-0001020eed82.html>

2 problem(s) in your installed packages found.

You are advised to update or deinstall the affected package(s)
immediately.
-  +- 1/8: Charlie Root          madman security check output                    -- (97%)
```

ports/net/gaim> - nectar@madman (1)

```
madman ports/net/gaim> make install

Gaim has the following tunable option(s):
        WITH_SILC               Build with Secure Internet Live Conferencing (SILC)
        WITHOUT_GTKSPELL        Turns off spell checking
        WITHOUT_AUDIO           Disable audio support
        WITH_GNUTLS             Enable GNUTLS encryption support
        WITHOUT_GNUTLS          Disable GNUTLS encryption support
        WITHOUT_NSS             Disable Mozilla NSS encryption support
        TCL_VER                 Use Tcl/Tk (version)

===>  gaim-1.1.1 has known vulnerabilities:
=> gaim -- AIM/ICQ remote denial of service vulnerability.
   Reference: <http://www.FreeBSD.org/ports/portaudit/8b0e94cc-b5cd-11d9-a788-0001020eed82.html>
=> gaim -- remote DoS on receiving malformed HTML.
   Reference: <http://www.FreeBSD.org/ports/portaudit/142353df-b5cc-11d9-a788-0001020eed82.html>
=> gaim -- jabber remote crash.
   Reference: <http://www.FreeBSD.org/ports/portaudit/ecf68408-a9f5-11d9-a788-0001020eed82.html>
=> gaim -- remote DoS on receiving certain messages over IRC.
   Reference: <http://www.FreeBSD.org/ports/portaudit/ec09baa3-a9f5-11d9-a788-0001020eed82.html>
=> gaim -- remote DoS on receiving malformed HTML.
   Reference: <http://www.FreeBSD.org/ports/portaudit/3fa2b372-a9f5-11d9-a788-0001020eed82.html>
=> Please update your ports tree and try again.
*** Error code 1

Stop in /1/home/nectar/ports/net/gaim.
madman ports/net/gaim>
```

VuXML document format

- XML 1.0 + Namespaces: Unicode, tags, attributes
- DTD for documentation and validation
- W3C Modularization of XHTML
- One document per package collection is typical

VuXML document format

- Top element is <vuxml>
- Elements are in http://www.vuxml.org/apps/vuxml-1 namespace
- Structure is record-like
- No sorting order defined
  - But conventionally new entries go at the top

<vuxml>

```
<vuxml xmlns="http://www.vuxml.org/apps/vuxml-1">
  <vuln ...
  <vuln ...
    .
    .
    .
</vuxml>
```

- Contains <vuln> elements
- version attribute, may be "1.0" or "1.1"

<vuln>

- Describes one vulnerability or exposure
  - 1 or more software package names, and 1 or more versions
  - Uniquely identified by VID (vuln ID)

<vuln>

```
<vuln vid="3374d8bd-fc85-4a51-9063-edf11503963f">
  <topic>fastquuxd -- authentication bypass<topic>
  <affects ...
  <description ...
  <references ...
  <dates ...
</vuln>
```

vid attribute is UUID; mandatory

- see e.g. *uuidgen(1)* on FreeBSD or Max OS X

<topic> contains a brief description; this and other elements are mandatory

- but maybe <cancelled> instead

<affects>

- Enumerates software package names and versions affected
  - <package> versus <system>
  - one or more <name> elements
  - followed by one or more <range> elements

<affects>

```
<affects>
  <package>
    <name>postgresql</name>
    <name>postgresql-server</name>
    <name>ja-postgresql</name>
    <range><lt>7.3.9</lt></range>
    <range><gt>7.4.*</gt><lt>7.4.7</lt></range>
    <range><gt>8.*</gt><lt>8.0.1</lt></range>
  </package>
  <package>
    <name>postgresql-devel</name>
    <range><le>8.0.1,1</le></range>
  </package>
</affects>
```

Affected packages

		ja-postgresql	<	7.3.9
7.4.*	<	ja-postgresql	<	7.4.7
8.*	<	ja-postgresql	<	8.0.1
		postgresql	<	7.3.9
7.4.*	<	postgresql	<	7.4.7
8.*	<	postgresql	<	8.0.1
		postgresql-server	<	7.3.9
7.4.*	<	postgresql-server	<	7.4.7
8.*	<	postgresql-server	<	8.0.1
		postgresql-devel	<=	8.0.1,1

- <eq>, <lt>, <le>, <gt>, <ge> specify version intervals
- Syntax of names and versions are not specified by VuXML; depends upon the package collection

<description>

- Rich description of the issue
- Contains an XHTML <body> element
- W3C "Modularization of XHTML"

XHTML modules included

text	hypertext
list	image
table	struct

<description>

```
<description>
  <body xmlns="http://www.w3.org/1999/xhtml">
    <p>Kevin Finisterre discovered bugs in perl's I/O debug support:</p>
    <ul>
      <li>The environmental variable PERLIO_DEBUG is honored even
        by the set-user-ID perl command (usually
        named <code>sperl</code> or <code>suidperl</code>).  As a
        result, a local attacker may be able to gain elevated
        privileges. <em>(CAN-2005-0155)</em></li>
      <li>A buffer overflow may occur in threaded versions of perl
        when the full pathname of the script being executed is
        very long. <em>(CAN-2005-0156)</em>.</li>
    </ul>
    <p><strong>Note:</strong> By default, no set-user-ID perl
      binary is installed.  An administrator must enable it
      manually at build time with the <code>ENABLE_SUIDPERL</code>
      port flag.</p>
  </body>
</description>
```

```
<description>
  <body xmlns="http://www.w3.org/1999/xhtml">
    <p>Giovanni Delvecchio reports:</p>
    <blockquote cite="http://www.zone-h.org/advisories/read/id=6503">
      <p>Opera for linux uses "kfmclient exec" as "Default
        Application" to handle saved files.  This could be used by
        malicious remote users to execute arbitrary shell commands
        on a target system.</p>
    </blockquote>
  </body>
</description>
```

<references>

- At least one reference must be present
- Different kinds of references have different elements
- Additional reference types are expected in later versions of VuXML

```
<references>
  <cvename ...>
  <url ...>
  <mlist ...>
    .
    .
    .
</references>
```

<url>

```
<url>https://bugzilla.mozilla.org/show_bug.cgi?id=288688</url>

<url>http://www.kde.org/info/security/advisory-20050316-1.txt</url>

<url>http://www.idefense.com/application/poi/display?
id=157&amp;type=vulnerabilities&amp;flashstatus=false</url>
```

- Universal Resource Locator.
- This resource type should only be used when none of the others apply.

<mlist>

```
<mlist msgid="200504120226.10559.pluf@7a69ezine.org">http://
marc.theaimsgroup.com/?l=bugtraq&amp;m=111331593310508</mlist>

<mlist>http://lists.freedesktop.org/pipermail/uim/2005-February/
000996.html</mlist>

<mlist msgid="412239E7.1070807@freebsd.lublin.pl">http://
lists.netsys.com/pipermail/full-disclosure/2004-August/025418.html</
mlist>
```

- An archived mailing list posting.
- The content is a URL.
- An optional msgid attribute may be present.

<cvename>

```
<cvename>CAN-2005-0709</cvename>

<cvename>CAN-2003-0965</cvename>

<cvename>CVE-2000-0442</cvename>
```

- The CVE name assigned by MITRE's Common Vulnerabilities and Exposures project.
- Probably actually a candidate.

<bid>

```
<bid>12615</bid>

<bid>9129</bid>

<bid>1241</bid>
```

- A SecurityFocus.com Bug ID.
- aka Bugtraq ID

US-CERT

```
<certsa>CA-2004-01</certsa>
<certvu>125598</certvu>
<uscertsa>SA02-300A</uscertsa>
<uscertta>TA04-356A</uscertta>
```

This one is fake: US-CERT has only issued CSAs for Microsoft products

- US-CERT (formerly CERT/CC) resources
- Security Advisories
- Vulnerability Notes
- Cyber Security Alerts, Technical Cyber Security Alerts

FreeBSD

```
<freebsdsa>SA-04:15.syscons</freebsdsa>
<freebsdsa>SA-04:05.openssl</freebsdsa>

   <freebsdpr>ports/56006</freebsdpr>
   <freebsdpr>ports/46613</freebsdpr>
```

- Security Advisories
- Problem Reports (PRs)

<dates>

```
<dates>
  <discovery>2005-04-11</discovery>
  <entry>2005-04-13</entry>
  <modified>2005-04-20</modified>
</dates>
```

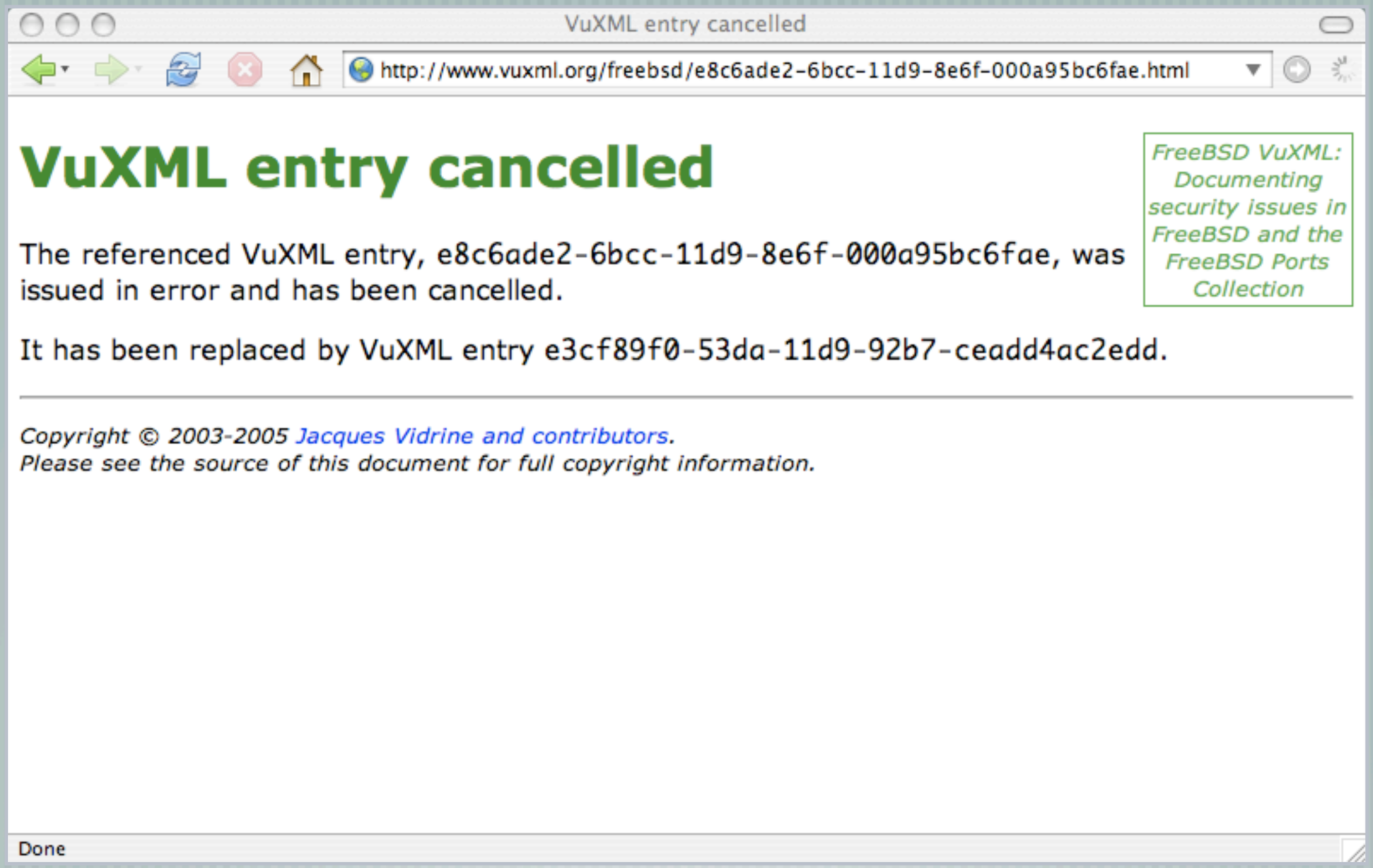
- <discovery>, date first publicly disclosed
- <entry>, date added to this document
- <modified>, date of most recent change

<cancelled>

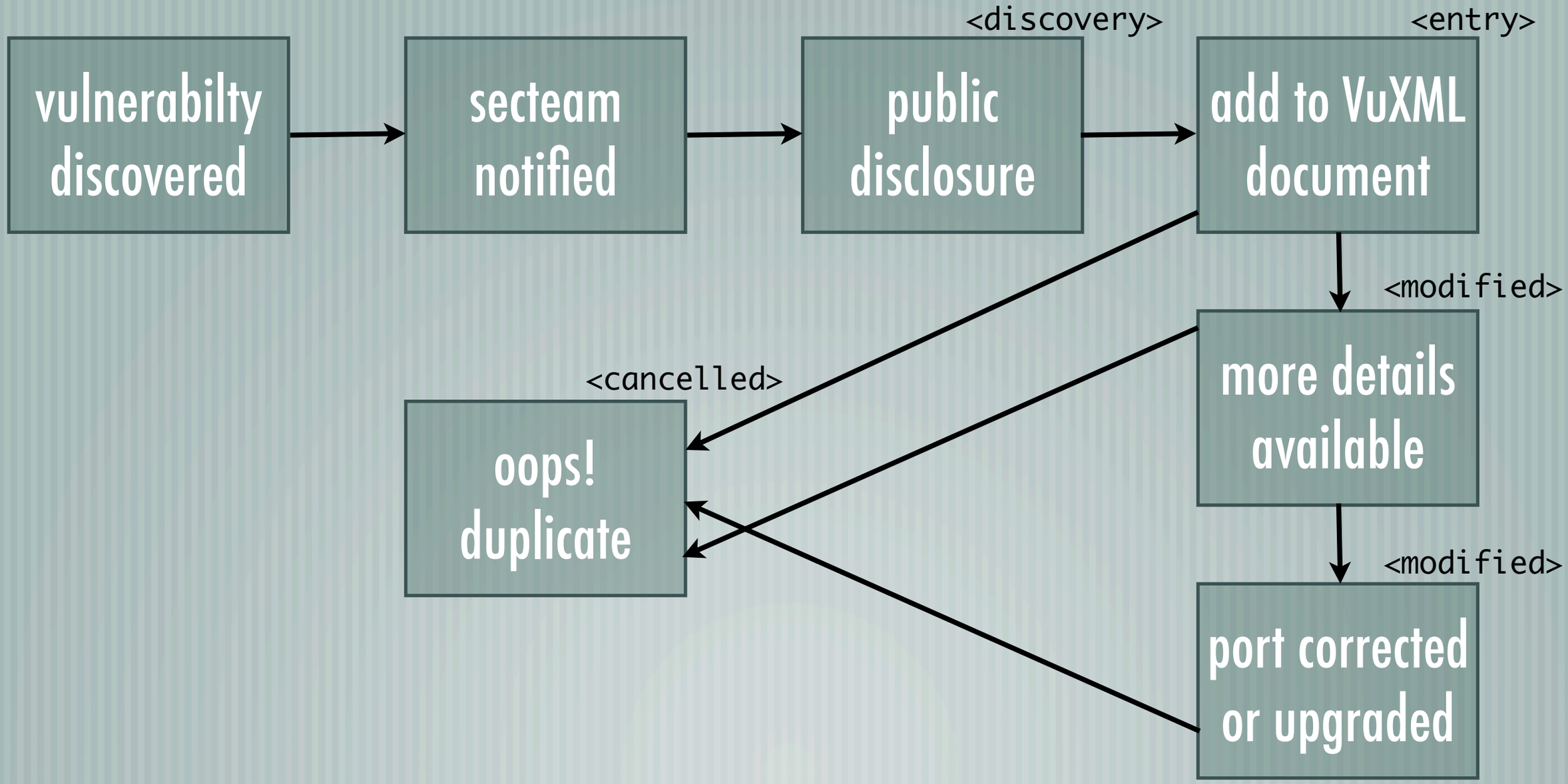
```
<vuln vid="e8c6ade2-6bcc-11d9-8e6f-000a95bc6fae">
  <cancelled superseded="e3cf89f0-53da-11d9-92b7-ceadd4ac2edd" />
</vuln>
```

- When a <vuln> is issued in error, it's content is replaced by a single <cancelled> element.
- An optional superseded attribute is useful for duplicates
- Why not just remove the <vuln>?
  - Processing tools may need to take some action

<cancelled>


VuXML entry cancelled
http://www.vuxml.org/freebsd/e8c6ade2-6bcc-11d9-8e6f-000a95bc6fae.html
VuXML entry cancelled
The referenced VuXML entry, e8c6ade2-6bcc-11d9-8e6f-000a95bc6fae, was issued in error and has been cancelled.
It has been replaced by VuXML entry e3cf89f0-53da-11d9-92b7-ceadd4ac2edd.
FreeBSD VuXML: Documenting security issues in FreeBSD and the FreeBSD Ports Collection
Copyright © 2003-2005 Jacques Vidrine and contributors.
Please see the source of this document for full copyright information.
Done

VuXML entry time line



Tips for making entries

FreeBSD specific

- Install ports/security/vuxml (the VuXML DTDs)
- The VuXML document is at ports/security/vuxml/vuln.xml
- Use a UTF-8-capable editor. I usually use VIM, even on ISO-8859 terminals.
- Do not use XHTML entities, only XML entities and character references. UTF-8 is preferred over character references.

Tips for making entries

- Start with "cd /usr/ports/security/vuxml"
- Get a template with "make newentry"
- Use <blockquote> liberally
- Check structure with "make validate"
- Find package names and versions in http://people.freebsd.org/~nectar/package-names.txt.bz2

Tips for making entries

- Find more notes and tips at http://simon.nitro.dk/vuxml.html
- Ports committers should commit directly. Others can bug a port committer or email <security@FreeBSD.org>.
- When submitting changes to **existing entries**, please send as a diff
- But when submitting **new entries**, just send the <vuln> element

Tool makers

- Versioning.
- Reference handling.
- Entities.
- Dates.

VuXML.org

Visit VuXML.org!

- Convenient access to contents of FreeBSD and OpenBSD VuXML documents.
- Official FreeBSD URLs begin with http://vuxml.freebsd.org/
- RSS syndication: your web site, Firefox, Thunderbird, Safari

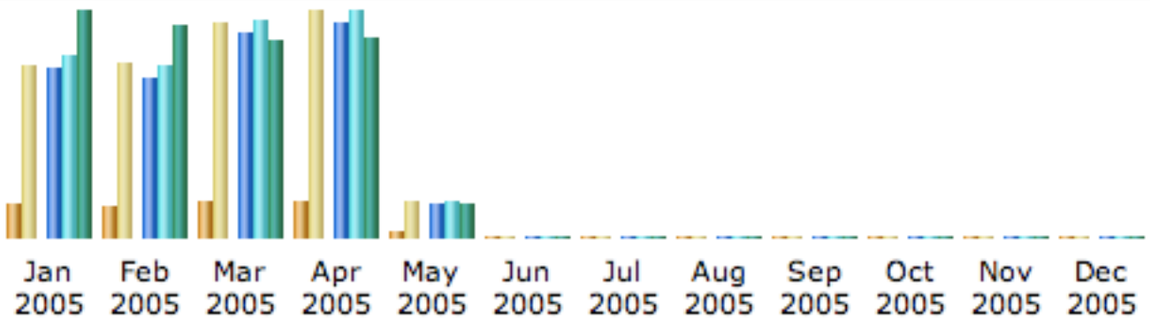
Site statistics

Summary

	First visit	Summary			Last visit
	01 Apr 2005 - 00:00	**Month Apr 2005**			30 Apr 2005 - 23:59
	Unique visitors	Number of visits	Pages	Hits	Bandwidth
Viewed traffic *	**6332**	**39128** (6.17 visits/visitor)	**120373** (3.07 pages/visit)	**127278** (3.25 hits/visit)	**778.73 MB** (20.37 KB/visit)
Not viewed traffic *			**47533**	**47559**	**131.42 MB**

* Not viewed trafic is trafic generated by robots, worms or answers with special HTTP status code.

Monthly history



Month	Unique visitors	Number of visits	Pages	Hits	Bandwidth
Jan 2005	5890	29727	95467	103002	876.98 MB
Feb 2005	5356	30413	90115	96996	819.64 MB
Mar 2005	6242	37312	115353	122490	769.58 MB
Apr 2005	6332	39128	120373	127278	778.73 MB

Total: 1574 different pages-url	Viewed
/freebsd/rss.xml	58371
/openbsd/rss.xml	24225
/freebsd/	11610
/openbsd/	4440
/dtd/vuxml-1/vuxml-11.dtd	3546
/dtd/vuxml-1/vuxml-model-11.mod	3521
/freebsd/22f00553-a09d-11d9-a788-0001020eed82.html	428
/	406
/freebsd/index-pkg.html	195
/freebsd/18e5428f-ae7c-11d9-837d-000e0c2e438a.html	176
/openbsd/be6057f4-9ecf-11d9-82a1-00065bd5b0b6.html	167
/freebsd/06f142ff-4df3-11d9-a9e7-0001020eed82.html	166
/freebsd/07f3fe15-a9de-11d9-a788-0001020eed82.html	155
/openbsd/c6f452e8-b00a-11d9-825c-00065bd5b0b6.html	134
/openbsd/99158684-a791-11d9-93dc-00065bd5b0b6.html	132
/freebsd/ef410571-a541-11d9-a788-0001020eed82.html	132
/freebsd/396ee517-a607-11d9-ac72-000bdb1444a4.html	126

VuXML contributors

Contributors to a VuXML document or VuXML.org

http://www.vuxml.org/freebsd/contributors.html
http://www.vuxml.org/openbsd/contributors.html

Matthias Andree	Hye-Shik Chang (장혜식)	Joe Marcus Clarke	Brooks Davis
Alex Dupre	Oliver Eikemeier	Josef El-Rayes	Frankye Fattarelli
Shane Kinney	Shinichiro Komatsu (小松晋一朗)	Hideyuki Kurashina (倉品英行)	Clement Laforet
Xin Li (李鑫)	Kang Liu (刘亢)	Remko Lodder	Nobutaka Mantani (萬谷暢崇)
Robert Nagy	Simon Nielsen	Devon O'Dell	Jon Passki
Hiroki Sato (佐藤広生)	Thomas-Martin Seck	Lev Serebryakov	Dag-Erling Smørgrav
Munechika Sumikawa (角川宗近)	Christian Weisgerber	Jared Wilson	

Want to help?

- Update/create new VuXML entries for OpenBSD or FreeBSD
- Encourage other projects to use VuXML, e.g. NetBSD, Fink
- VuXML editing applications, including web-based submission tool
- Automated port maintainer nagger
- More system auditing tools