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>
</vuxml>
Let's take a peek

unace -- multiple vulnerabilities

**Affected packages**
unace < unace-1.2b_2

**Details**

<table>
<thead>
<tr>
<th>VuXML ID</th>
<th>1d3a2737-7eb7-11d9-acf7-000854d03344</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery</td>
<td>2005-02-14</td>
</tr>
<tr>
<td>Entry</td>
<td>2005-02-22</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>CVE Name</th>
<th>CAN-2005-0160</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE Name</td>
<td>CAN-2005-0161</td>
</tr>
</tbody>
</table>
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

```
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</topic>
  <affects>
    <package>
      <name>php4</name>
    </package>
    <name>php4-cgi</name>
  </affects>
</vuln>
```

```
VuXML.org

OpenBSD VuXML - entry date index

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 be seen at anoncvs@beastie.hu:/cvs, file vuxml/vuln.x

entry date index

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

<table>
<thead>
<tr>
<th>Entered</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005-05-05</td>
<td>leafnode -- denial of service</td>
</tr>
<tr>
<td>2005-05-01</td>
<td>ImageMagick -- ReadPNImage() heap overflow vul</td>
</tr>
<tr>
<td>2005-04-27</td>
<td>xv -- multiple buffer overflows</td>
</tr>
<tr>
<td>2005-04-12</td>
<td>rsnapshot -- local privilege escalation</td>
</tr>
<tr>
<td>2005-04-07</td>
<td>gaim -- multiple vulnerabilities</td>
</tr>
<tr>
<td>2005-04-04</td>
<td>php4 -- multiple vulnerabilities</td>
</tr>
<tr>
<td>2005-04-04</td>
<td>php5 -- multiple vulnerabilities</td>
</tr>
<tr>
<td>2005-05-05</td>
<td>gnupg -- OpenPGP protocol attack</td>
</tr>
<tr>
<td>2005-03-27</td>
<td>tiff -- multiple vulnerabilities</td>
</tr>
<tr>
<td>2005-03-23</td>
<td>jabberd -- multiple vulnerabilities</td>
</tr>
<tr>
<td>2005-03-22</td>
<td>grip -- CDDDB response multiple matches buffer overflow vulnerability</td>
</tr>
</tbody>
</table>
VuXML.org

VuXML: imlib -- xpm heap buffer overflows and integer overflows

http://www.vuxml.org/freebsd/2001103a-6bbd-11d9-851d-000a95bc6fae.html

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.

The flaws also affect imlib2.

References

- **Bugtraq ID**: 11830
- **CVE Name**: CAN-2004-1625
- **CVE Name**: CAN-2004-1725

VuXML.org

**CAN-2005-0704**

This CVE name corresponds to:

<table>
<thead>
<tr>
<th>Entered</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005-03-14</td>
<td>ethereal -- multiple protocol dissectors vulnerabilities</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Type</th>
<th>Candidate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>CAN-2005-0704</td>
</tr>
<tr>
<td>Phase</td>
<td>Assigned(20050309)</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Source</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>GENTOO</td>
<td>GLSA-200503-16</td>
</tr>
<tr>
<td>MANDRAKE</td>
<td>MDKSA-2005-053</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>VuXML ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ec09baa3-a9f5-11d9-a788-0001020eed82</td>
<td>gaim -- remote DoS on receiving certain messages over IRC</td>
</tr>
</tbody>
</table>

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_kill, irc_msg_mode, irc_msg_part, irc_msg_quit, (2) remote...
What is VuXML?                  Jacques Vidrine <nectar@FreeBSD.org>

vxquery

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, vxxml, xhtml, xhtml-files
What is VuXML?                  Jacques Vidrine <nectar@FreeBSD.org>
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
<?xml version="1.0" encoding="UTF-8"?>
<vuxml xmlns="http://www.vuxml.org/apps/vuxml-1">
  <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 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>
  <package>
    <name>postgresql</name>
    <name>postgresql-server</name>
    <name>ja-postgresql</name>
    <range><lt>7.3.9</lt></range>
    <range><gt>7.4.7</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>

<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"

<table>
<thead>
<tr>
<th>XHTML modules included</th>
</tr>
</thead>
<tbody>
<tr>
<td>text</td>
</tr>
<tr>
<td>hypertext</td>
</tr>
<tr>
<td>list</td>
</tr>
<tr>
<td>image</td>
</tr>
<tr>
<td>table</td>
</tr>
<tr>
<td>struct</td>
</tr>
</tbody>
</table>
Kevin Finisterre discovered bugs in perl's I/O debug support:

- The environmental variable PERLIO_DEBUG is honored even by the set-user-ID perl command (usually named `sperl` or `suidperl`). As a result, a local attacker may be able to gain elevated privileges. *(CAN-2005-0155)*

- A buffer overflow may occur in threaded versions of perl when the full pathname of the script being executed is very long. *(CAN-2005-0156)*

Note: By default, no set-user-ID perl binary is installed. An administrator must enable it manually at build time with the `ENABLE_SUIDPERL` port flag.

Giovanni Delvecchio reports:

- 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.
At least one reference must be present

Different kinds of references have different elements

Additional reference types are expected in later versions of VuXML
Universal Resource Locator.

This resource type should only be used when none of the others apply.

[url]https://bugzilla.mozilla.org/show_bug.cgi?id=288688[/url]


An archived mailing list posting.
The content is a URL.
An optional msgid attribute may be present.
The CVE name assigned by MITRE's Common Vulnerabilities and Exposures project.

Probably actually a candidate.
&lt;bid&gt;

&lt;bid&gt;12615&lt;/bid&gt;
&lt;bid&gt;9129&lt;/bid&gt;
&lt;bid&gt;1241&lt;/bid&gt;

A SecurityFocus.com Bug ID.

aka Bugtraq ID
This one is fake: US-CERT has only issued CSAs for Microsoft products.
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>
  <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
VuXML entry time line

- Vulnerability discovered
- Secteam notified
- Public disclosure
- Add to VuXML document
- More details available
- Port corrected or upgraded
- Oops! Duplicate
- Cancelled
- Discovery
- Entry
- Modified
Tips for making entries

- 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.
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

<table>
<thead>
<tr>
<th>First visit</th>
<th>Summary</th>
<th>Last visit</th>
</tr>
</thead>
<tbody>
<tr>
<td>01 Apr 2005</td>
<td>Month Apr 2005</td>
<td>30 Apr 2005</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Viewed traffic</th>
<th>Number of visits</th>
<th>Pages</th>
<th>Hits</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unique visitors</td>
<td>6332</td>
<td>39128</td>
<td>120373</td>
<td>127278</td>
</tr>
<tr>
<td>(6.17 visits/visitor)</td>
<td>(3.07 pages/visit)</td>
<td>(3.25 hits/visit)</td>
<td>(20.37 KB/visit)</td>
<td></td>
</tr>
<tr>
<td>Not viewed traffic</td>
<td>47533</td>
<td>47559</td>
<td>131.42 MB</td>
<td></td>
</tr>
</tbody>
</table>

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

Monthly history

<table>
<thead>
<tr>
<th>Month</th>
<th>Unique visitors</th>
<th>Number of visits</th>
<th>Pages</th>
<th>Hits</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 2005</td>
<td>5890</td>
<td>29727</td>
<td>95467</td>
<td>103002</td>
<td>876.98 MB</td>
</tr>
<tr>
<td>Feb 2005</td>
<td>5356</td>
<td>30413</td>
<td>90115</td>
<td>96996</td>
<td>819.64 MB</td>
</tr>
<tr>
<td>Mar 2005</td>
<td>6242</td>
<td>37312</td>
<td>115353</td>
<td>122490</td>
<td>769.58 MB</td>
</tr>
<tr>
<td>Apr 2005</td>
<td>6332</td>
<td>39128</td>
<td>120373</td>
<td>127278</td>
<td>778.73 MB</td>
</tr>
</tbody>
</table>

Total: 1574 different pages-url

- /freebsd/rss.xml: 58371
- /openbsd/rss.xml: 24225
- /freebsd/: 11610
- /openbsd/: 4440
- /DTD/vuXML-1/vuXML-1.dtd: 3546
- /freebsd/22f00553-a09d-11d9-a788-00010200ed82.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-a9e7-00010200ed82.html: 166
- /freebsd/07f3fe15-a9de-11d9-a788-00010200ed82.html: 155
- /openbsd/c6f452e8-b00a-11d9-825c-00065bd5b0b6.html: 134
- /openbsd/99158684-a791-11d9-93dc-00065bd5b0b6.html: 132
- /freebsd/ef410571-a541-11d9-a788-00010200ed82.html: 132
- /freebsd/396ee517-a607-11d9-ac72-000b0b1444a4.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

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