

# Adventures in Open Source Software: Dealing with Security



## Life in the pkgsrc security team

By Sevan Janiyan



# What is pkgsrc

Cross platform packaging system

23 listed platforms in 2015Q3 release notes

Strive to keep local changes minimal (co-ordinate with upstream)

Focus on portability

Limited arch cross-compile support (NetBSD only)

Somewhat consistent build across platforms however

Easily auditable and adaptable





## Browse pkgsrc

### + virtual

archivers  
audio  
benchmarks  
biology  
cad  
chat  
comms  
converters  
cross  
crosspkgtools  
databases  
devel  
doc  
editors  
emulators  
filesystems  
finance  
fonts  
games  
geography  
graphics  
ham  
inputmethod  
lang  
mail  
math  
mbone  
meta-pkgs  
misc  
multimedia  
net  
news  
parallel  
pkgtools  
print

Branch: [CURRENT](#), [pkgsrc-2015Q3](#), [pkgsrc-2015Q2](#), [pkgsrc-2015Q1](#), ...

### 2015-11-19 / **NEW PACKAGE** (1.3.1)

[graphics/py-graphviz](#)

**COMMENT:** Python interface to the Graphviz package

**MAINTAINER(S):** [helgoman](#)

### 2015-11-19 / **UPDATED** (15.2nb1 => 15.2nb2)

[multimedia/kodi](#)

**COMMENT:** Open source software media center

**MAINTAINER(S):** [jmcneill](#)

### 2015-11-19 / **UPDATED** (2.9.3 => 3.0)

[www/moodle](#)

**COMMENT:** Course management system based on social constructionism

**MAINTAINER(S):** [wenheping](#)

### 2015-11-19 / **UPDATED** (6.29 => 6.32)

[www/p5-Mojolicious](#)

**COMMENT:** Perl web framework: The Web In A Box!

**MAINTAINER(S):** [pkgsrc-users](#)

### 2015-11-19 / **UPDATED** (3.6 => 3.6nb1)

## Start Download

File size: 487KB.  
OS: MacOSX.  
Rating: 5.0  
Stars - ZipDevil





## Browse pkgsrc

### + virtual

archivers  
audio  
benchmarks  
biology  
cad  
chat  
comms  
converters  
cross  
crosspkgtools  
databases  
devel  
doc  
editors  
emulators  
filesystems  
finance  
fonts  
games  
geography  
graphics  
ham  
inputmethod  
lang  
mail  
math  
mbone  
meta-pkgs  
misc  
► **multimedia**  
  ► **kodi**  
net  
news  
parallel  
pkgtools

[./multimedia/kodi](#), *Open source software media center*

[ [CVSweb](#) ] [ [Homepage](#) ] [ [RSS](#) ] [ [Required by](#) ] [ [Add to tracker](#) ]

**Branch:** CURRENT, **Version:** 15.2nb2, **Package name:** kodi-15.2nb2, **Maintainer:** [jmcneill](#)

Kodi (formerly known as XBMC) is an award-winning free and open source (GPL) software media center for playing videos, music, pictures, games, and more. Kodi features a 10-foot user interface for use with televisions and remote controls. It allows users to play and view most videos, music, podcasts, and other digital media files from local and network storage media and the internet.

### Required to run:

[[sysutils/desktop-file-utils](#)] [[sysutils/dbus](#)] [[textproc/libxml2](#)] [[textproc/libxslt](#)] [[converters/fribidi](#)] [[www/curl](#)]  
[[misc/libcdio](#)] [[graphics/MesaLib](#)] [[graphics/hicolor-icon-theme](#)] [[graphics/jasper](#)] [[graphics/tiff](#)] [[graphics/freetype2](#)]  
[[graphics/png](#)] [[graphics/glew](#)] [[multimedia/libmpeg2](#)] [[multimedia/libogg](#)] [[archivers/lzo](#)] [[archivers/unzip](#)]  
[[archivers/zip](#)] [[audio/libmpcdec](#)] [[audio/libmodplug](#)] [[audio/libao](#)] [[audio/libao-oss](#)] [[audio/libvorbis](#)] [[audio/taglib](#)]  
[[fonts/fontconfig](#)] [[net/avahi](#)] [[security/libssh](#)] [[devel/boost-libs](#)] [[devel/pcre](#)] [[devel/libusb](#)] [[devel/libstdc++](#)]

Buy   
**Balancing Scooter**  
Buy Balancing Electric Scooter, Top Quality, Free Shipping, Buy.






















## pkgsrc/multimedia/kodi/patches/

Click on a directory to enter that directory. Click on a file to display its revision history and to get a chance to display diffs between revisions.

Current directory: [\[cvs.NetBSD.org\]](#) / [pkgsrc](#) / [multimedia](#) / [kodi](#) / [patches](#)

File	Rev.	Age	Author	Last log entry
 <a href="#">Parent Directory</a>				
 <a href="#">patch-Makefile.in</a>	<a href="#">1.1</a>	2 days	jmcneill	Initial import of kodi-15.2 Kodi (formerly known as XBMC) is an award-winning f...
 <a href="#">patch-bootstrap</a>	<a href="#">1.1</a>	2 days	jmcneill	Initial import of kodi-15.2 Kodi (formerly known as XBMC) is an award-winning f...
 <a href="#">patch-codegenerator.mk</a>	<a href="#">1.1</a>	2 days	jmcneill	Initial import of kodi-15.2 Kodi (formerly known as XBMC) is an award-winning f...
 <a href="#">patch-configure.ac</a>	<a href="#">1.3</a>	2 days	jmcneill	enable NEON for armv7
 <a href="#">patch-lib_cximage-6.0_CxImage_DllInterface.cpp</a>	<a href="#">1.1</a>	2 days	jmcneill	Initial import of kodi-15.2 Kodi (formerly known as XBMC) is an award-winning f...
 <a href="#">patch-lib_cximage-6.0_CxImage_ximage.h</a>	<a href="#">1.1</a>	2 days	jmcneill	Initial import of kodi-15.2 Kodi (formerly known as XBMC) is an award-winning f...
 <a href="#">patch-lib_cximage-6.0_CxImage_ximainfo.cpp</a>	<a href="#">1.1</a>	2 days	jmcneill	Initial import of kodi-15.2 Kodi (formerly known as XBMC) is an award-winning f...
 <a href="#">patch-m4_xbmc_arch.m4</a>	<a href="#">1.2</a>	2 days	christos	fix amd64
 <a href="#">patch-xbmc_GUIInfoManager.cpp</a>	<a href="#">1.1</a>	2 days	jmcneill	Initial import of kodi-15.2 Kodi (formerly known as XBMC) is an award-winning f...
 <a href="#">patch-xbmc_Makefile.in</a>	<a href="#">1.1</a>	2 days	jmcneill	Initial import of kodi-15.2 Kodi (formerly known as XBMC) is an award-winning f...
 <a href="#">patch-xbmc_Util.cpp</a>	<a href="#">1.1</a>	2 days	jmcneill	Initial import of kodi-15.2 Kodi (formerly known as XBMC) is an award-winning f...
 <a href="#">patch-lib_cximage-6.0_CxImage_ximage.h</a>				Initial import of kodi-15.2 Kodi (formerly known as XBMC) is an award-winning f...

Open "cvsweb.netbsd.org/bsdweb.cgi/pkgsrc/multimedia/kodi/patches/patch-lib\_cximage-6.0\_CxImage\_ximage.h" in a new tab



[Return to patch-Makefile.in](#) CVS log

Up to [\[cvs.NetBSD.org\]](#) / [pkgsrc](#) / [multimedia](#) / [kodi](#) / [patches](#)

File: [\[cvs.NetBSD.org\]](#) / [pkgsrc](#) / [multimedia](#) / [kodi](#) / [patches](#) / [patch-Makefile.in](#) ([download](#))

Revision 1.1, Tue Nov 17 14:56:07 2015 UTC (2 days, 3 hours ago) by *jmcneill*

Branch: **MAIN**

CVS Tags: **HEAD**

Initial import of kodi-15.2

Kodi (formerly known as XBMC) is an award-winning free and open source (GPL) software media center for playing videos, music, pictures, games, and more. Kodi features a 10-foot user interface for use with televisions and remote controls. It allows users to play and view most videos, music, podcasts, and other digital media files from local and network storage media and the internet.

\$NetBSD: patch-Makefile.in,v 1.1 2015/11/17 14:56:07 jmcneill Exp \$

```
--- Makefile.in.orig      2015-10-19 06:31:15.000000000 +0000
+++ Makefile.in
@@ -169,6 +169,10 @@ ifeq ($(findstring freebsd,@ARCH@),freeb
    DIRECTORY_ARCHIVES += xbmc/freebsd/freebsd.a
    endif

+ifeq ($(findstring netbsd,@ARCH@),netbsd)
+DIRECTORY_ARCHIVES += xbmc/freebsd/freebsd.a
+endif
+
    ifeq (@HAVE_XBMC_NONFREE@,1)
    DIRECTORY_ARCHIVES += lib/UnrarXLib/UnrarXLib.a
    endif
@@ -436,6 +440,11 @@ ifeq ($(findstring freebsd,@ARCH@),freeb
    DYNOBJSXBMC+= xbmc/freebsd/freebsd.a
    endif

+ifeq ($(findstring netbsd,@ARCH@),netbsd)
+DYNOBJSXBMC+= xbmc/freebsd/freebsd.a
+endif
+
+
    ifeq (@USE_STATIC_FFMPEG@,1)
    FFMPEGOBJS = @FFMPEG_LIBDIR@/libavcodec.a \
                @FFMPEG_LIBDIR@/libavfilter.a \
```



# Advisories





## Common Vulnerabilities and Exposures

*The Standard for Information Security Vulnerability Names*

**CVE-IDs have a new format –\*\*[Learn more](#)\*\***

TOTAL CVE-IDs: **72805**

### About CVE

Terminology  
Documents  
FAQs

### CVE List

CVE-ID Syntax Change  
About CVE Identifiers  
Search CVE  
Search NVD  
Updates & RSS Feeds  
Request a CVE-ID

### CVE In Use

CVE-Compatible Products  
NVD for CVE Fix  
Information  
CVSS for Scoring CVE-IDs  
CVE Numbering  
Authorities (CNAs)

### News & Events

Calendar  
Free Newsletter

### Community

CVE Editorial Board

**CVE®** International in scope and free for public use, CVE is a dictionary of publicly known information security vulnerabilities and exposures.

CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.

## Widespread Use of CVE

- ▲ [CVE Numbering Authorities \(CNAs\)](#)
- ▲ [NVD \(National Vulnerability Database\)](#)
- ▲ [Vulnerability Scoring \(CVSS\)](#)
- ▲ [CVE-Compatible Products & Services](#)
- ▲ [Security Content Automation](#)
- ▲ [US-CERT Bulletins](#)
- ▲ [International Standard: Recommendation ITU-T X.1520 Common Vulnerabilities and Exposures \(CVE\), ITU-T CYBEX Series](#)
- ▲ [Vulnerability Management](#)
- ▲ [Patch Management](#)
- ▲ [Vulnerability Alerting](#)
- ▲ [Intrusion Detection](#)

### Latest News

New CVE Editorial Board Member for Red Hat

CVE Mentioned in Article about Joomla Vulnerabilities Affecting Millions of Websites on Ars Technica

CVE Identifier "CVE-2015-7645" Cited in Numerous Security Advisories and News Media References about a Zero-Day Adobe Flash Vulnerability

CVE Included in Cisco's Recently Updated Vulnerability Disclosure Process

Upcoming Changes to CVE

[More News »](#)



# Drupal Core - Critical - Multiple Vulnerabilities - SA-CORE-2015-003

Posted by [Drupal Security Team](#) on *August 19, 2015 at 7:27pm*

- Advisory ID: DRUPAL-SA-CORE-2015-003
- Project: [Drupal core](#)
- Version: 6.x, 7.x
- Date: 2015-August-19
- Security risk: 18/25 **Critical** AC:Complex/A:User/CI:All/II:All/E:Proof/TD:All
- Vulnerability: Cross Site Scripting, Access bypass, SQL Injection, Open Redirect, Multiple vulnerabilities

This security advisory fixes multiple vulnerabilities. See below for a list.

## Cross-site Scripting - Ajax system - Drupal 7

A vulnerability was found that allows a malicious user to perform a cross-site scripting attack by invoking `Drupal.ajax()` on a whitelisted HTML element.

This vulnerability is mitigated on sites that do not allow untrusted users to enter HTML.

Drupal 6 core is not affected, but see the similar advisory for the Drupal 6 contributed Ctools module: [SA-CONTRIB-2015-141](#).

## Cross-site Scripting - Autocomplete system - Drupal 6 and 7

A cross-site scripting vulnerability was found in the autocomplete functionality of forms. The requested URL is not sufficiently sanitized.

This vulnerability is mitigated by the fact that the malicious user must be allowed to upload files.

## SQL Injection - Database API - Drupal 7

A vulnerability was found in the SQL comment filtering system which could allow a user with elevated permissions to inject malicious code in SQL comments.

This vulnerability is mitigated by the fact that only one contributed module that the security team found uses the comment filtering system in a way that would trigger the vulnerability. That module requires you to have a very high level of access in order to perform the attack.

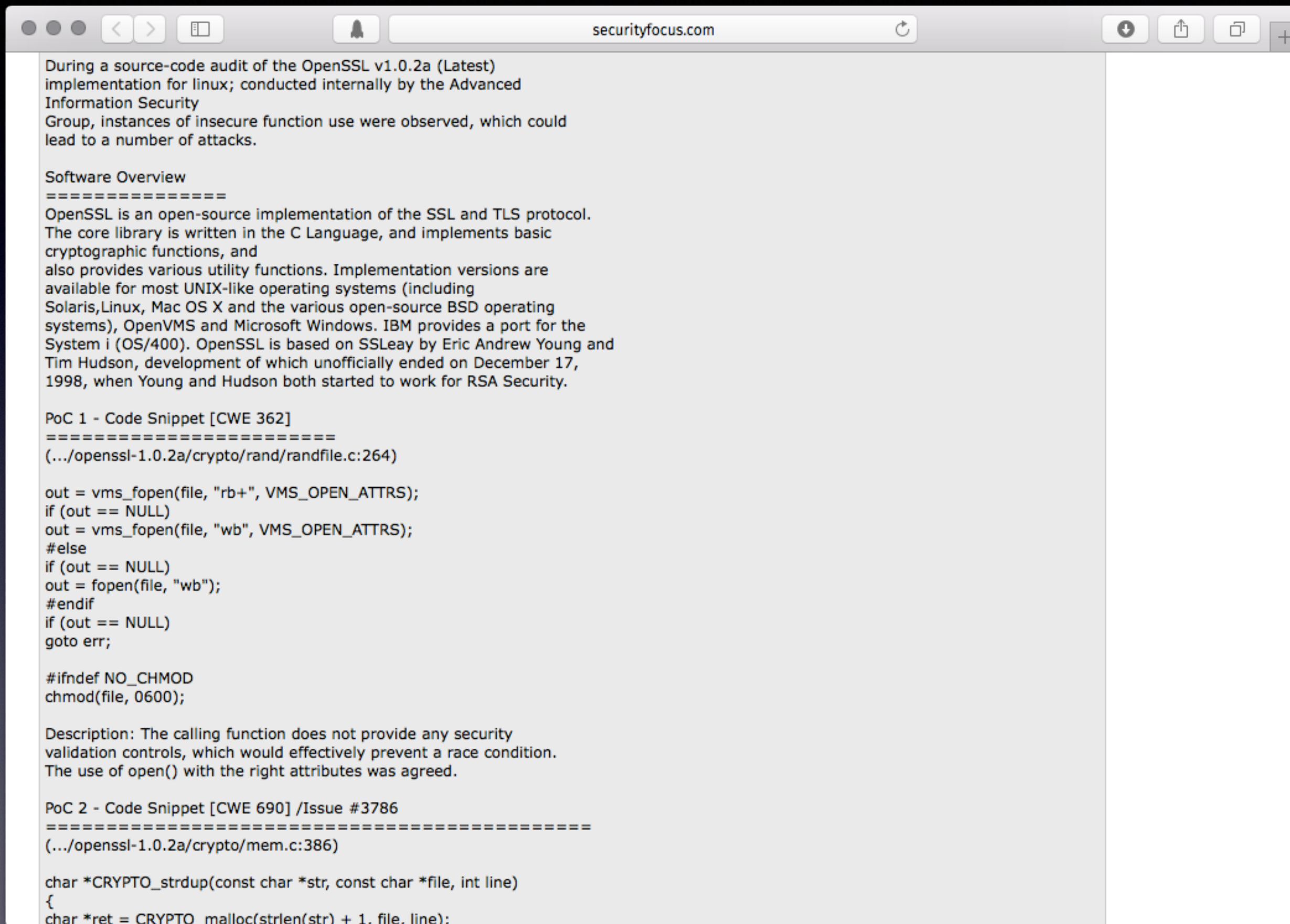


"We never contacted FreeBSD or NetBSD because we didn't spend enough time to check kame.net. To be honest NetBSD is a pain to deal with. To install FreeBSD or NetBSD takes hours I don't have. I got the offer to give a subversive anti-authoritarian talk at TA3M. I sent a friendly request to my colleagues. I wrote it up. My colleagues published the vulnerability to SourceForge. Now I'm doing the full disclosure and advertising necessary to get people to switch."

<https://www.altsci.com/ipsec/ipsec-tools-sa.html>



# Advanced Information Security Corp



The screenshot shows a web browser window with the address bar displaying "securityfocus.com". The page content is a security advisory. The first paragraph describes a source-code audit of OpenSSL v1.0.2a (Latest) for Linux, conducted internally by the Advanced Information Security Group, noting insecure function use that could lead to attacks. The second section, "Software Overview", provides a general description of OpenSSL as an open-source implementation of SSL and TLS. The third section, "PoC 1 - Code Snippet [CWE 362]", includes a C code snippet from rand/randfile.c:264 that demonstrates a race condition by using 'fopen' instead of 'open' with proper security attributes. The fourth section, "PoC 2 - Code Snippet [CWE 690] /Issue #3786", shows a C code snippet from mem.c:386 that demonstrates a memory allocation issue. The browser interface includes standard navigation buttons and a sidebar on the right.

During a source-code audit of the OpenSSL v1.0.2a (Latest) implementation for linux; conducted internally by the Advanced Information Security Group, instances of insecure function use were observed, which could lead to a number of attacks.

Software Overview  
=====

OpenSSL is an open-source implementation of the SSL and TLS protocol. The core library is written in the C Language, and implements basic cryptographic functions, and also provides various utility functions. Implementation versions are available for most UNIX-like operating systems (including Solaris, Linux, Mac OS X and the various open-source BSD operating systems), OpenVMS and Microsoft Windows. IBM provides a port for the System i (OS/400). OpenSSL is based on SSLeay by Eric Andrew Young and Tim Hudson, development of which unofficially ended on December 17, 1998, when Young and Hudson both started to work for RSA Security.

PoC 1 - Code Snippet [CWE 362]  
=====

(.../openssl-1.0.2a/crypto/rand/randfile.c:264)

```
out = vms_fopen(file, "rb+", VMS_OPEN_ATTRS);
if (out == NULL)
out = vms_fopen(file, "wb", VMS_OPEN_ATTRS);
#else
if (out == NULL)
out = fopen(file, "wb");
#endif
if (out == NULL)
goto err;
```

#ifndef NO\_CHMOD  
chmod(file, 0600);

Description: The calling function does not provide any security validation controls, which would effectively prevent a race condition. The use of open() with the right attributes was agreed.

PoC 2 - Code Snippet [CWE 690] /Issue #3786  
=====

(.../openssl-1.0.2a/crypto/mem.c:386)

```
char *CRYPTO_strdup(const char *str, const char *file, int line)
{
char *ret = CRYPTO_malloc(strlen(str) + 1, file, line);
```



oracle.com													
CVE#	Component	Protocol	Sub-component	Remote Exploit without Auth.?	CVSS VERSION 2.0 RISK (see <a href="#">Risk Matrix Definitions</a> )							Supported Versions Affected	Notes
					Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability		
CVE-2015-4835	Java SE, Java SE Embedded	Multiple	CORBA	Yes	10.0	Network	Low	None	Complete	Complete	Complete	Java SE 6u101, Java SE 7u85, Java SE 8u60, Java SE Embedded 8u51	See Note 1
CVE-2015-4881	Java SE, Java SE Embedded	Multiple	CORBA	Yes	10.0	Network	Low	None	Complete	Complete	Complete	Java SE 6u101, Java SE 7u85, Java SE 8u60, Java SE Embedded 8u51	See Note 1
CVE-2015-4843	Java SE, Java SE Embedded	Multiple	Libraries	Yes	10.0	Network	Low	None	Complete	Complete	Complete	Java SE 6u101, Java SE 7u85, Java SE 8u60, Java SE Embedded 8u51	See Note 1
CVE-2015-4883	Java SE, Java SE Embedded	Multiple	RMI	Yes	10.0	Network	Low	None	Complete	Complete	Complete	Java SE 6u101, Java SE 7u85, Java SE 8u60, Java SE Embedded 8u51	See Note 1
CVE-2015-4860	Java SE, Java SE Embedded	Multiple	RMI	Yes	10.0	Network	Low	None	Complete	Complete	Complete	Java SE 6u101, Java SE 7u85, Java SE 8u60, Java SE Embedded 8u51	See Note 1
CVE-2015-4805	Java SE, Java SE Embedded	Multiple	Serialization	Yes	10.0	Network	Low	None	Complete	Complete	Complete	Java SE 6u101, Java SE 7u85, Java SE 8u60, Java SE Embedded 8u51	See Note 1
CVE-2015-4844	Java SE, Java SE Embedded	Mutiple	2D	Yes	10.0	Network	Low	None	Complete	Complete	Complete	Java SE 6u101, Java SE 7u85, Java SE 8u60, Java SE Embedded 8u51	See Note 1



**\*\* RESERVED \*\*** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided



# package	type of exploit	URL
cfengine<1.5.3nb3	remote-root-shell	ftp://ftp.NetBSD.org/pub/NetBSD/security/advisories/NetBSD-SA2000-013.txt.asc
navigator<4.75	remote-user-access	http://www.cert.org/advisories/CA-2000-15.html
navigator<4.74	remote-user-shell	ftp://ftp.NetBSD.org/pub/NetBSD/security/advisories/NetBSD-SA2000-011.txt.asc
communicator<4.75	remote-user-access	http://www.cert.org/advisories/CA-2000-15.html
communicator<4.74	remote-user-shell	ftp://ftp.NetBSD.org/pub/NetBSD/security/advisories/NetBSD-SA2000-011.txt.asc
pine<4.30	remote-user-shell	http://www.securityfocus.com/bid/1709
pine<4.21nb1	denial-of-service	http://www.securityfocus.com/advisories/2646
imap-uw<4.7c6	denial-of-service	http://www.securityfocus.com/advisories/2646
screen<3.9.5nb1	local-root-shell	http://www.securityfocus.com/advisories/2634
ntop<1.1	remote-root-shell	http://www.securityfocus.com/advisories/2520
wu-ftp<2.6.1	remote-root-shell	ftp://ftp.NetBSD.org/pub/NetBSD/security/advisories/NetBSD-SA2000-010.txt.asc
wu-ftp<2.4.2b18.2	remote-root-shell	ftp://ftp.NetBSD.org/pub/NetBSD/security/advisories/NetBSD-SA1999-003.txt.asc
xlockmore<4.17	local-root-file-view	ftp://ftp.NetBSD.org/pub/NetBSD/security/advisories/NetBSD-SA2000-003.txt.asc
lsof<4.41	local-root-shell	ftp://ftp.NetBSD.org/pub/NetBSD/security/advisories/NetBSD-SA1999-005.txt.asc
wu-ftp<2.6.0	remote-root-shell	ftp://ftp.NetBSD.org/pub/NetBSD/security/advisories/NetBSD-SA1999-003.txt.asc
racoon<20001004a	local-root-file-view	http://mail-index.NetBSD.org/tech-net/2000/09/24/0000.html
global<3.56	remote-user-access	http://www.NetBSD.org/cgi-bin/query-pr-single.pl?number=11165
apache<1.3.14	remote-user-access	http://httpd.apache.org/dist/httpd/CHANGES_1.3
apache6<1.3.14	remote-user-access	http://httpd.apache.org/dist/httpd/CHANGES_1.3
thttpd<2.20	remote-user-access	http://www.dopesquad.net/security/advisories/20001002-thttpd-ssi.txt
bind<8.2.2.7	denial-of-service	http://www.isc.org/products/BIND/bind-security.html
gnupg<1.0.4	weak-authentication	http://www.gnupg.org/whatsnew.html#rn20001017

<ftp://ftp.netbsd.org/pub/NetBSD/packages/vulns/pkg-vulnerabilities>



# Project Websites





# ICU - International Components for Unicode

security

Search this site

## Navigation

### About ICU

- [ICU Home](#)
- [Download ICU](#)

### Demos & Tools

- [ICU4C Demos](#)
- [ICU Collation Demo](#)
- [ICU4J Demos](#)
- [Data Customizer](#)

### Documents

- [User Guide](#)
- [ICU FAQ](#)
- [ICU4J FAQ](#)
- [Docs & Papers](#)

### API References

#### Official Release

- [ICU4C \(56.1\)](#)
- [ICU4J \(56.1\)](#)

#### Latest Development Version

- [N/A](#)

### Data & Charts

- [Conversion Tables](#)
- [Feature Comparisons](#)
- [Performance & Size](#)

### Development

- [Project Information](#)
- [Design Docs](#)
- [Source Repository](#)
- [Processes](#)
- [Members-Only Area](#)

### Bugs & Contacts

- [Bugs](#)
- [Feature Requests](#)
- [Mailing Lists](#)
- [Feedback](#)
- [Sitemap](#)

## Related Websites

- [Unicode Consortium](#)
- [Common Locale Data](#)
- [IBM Open Source](#)
- [Globalize Your E-](#)

## Search results

Showing 1-7 of 7 results for **security**

### [Java 7 Support](#) Aug 2, 2011, 3:05 PM by Yoshito Umaoka

... Java Virtual Machine. This does not affect the host locale. If there is a **security** manager, its checkPermission method is called with a PropertyPermission("user.language", "write") permission before the ...

[Design Docs](#) > [Java 7 Support](#)

### [Download ICU 51](#) May 23, 2013, 9:10 PM by Steven R. Loomis

... folder when building with Visual Studio [ #10047] [ Fixed in 51.2] 2013-Apr-18: **Security** Vulnerabilities in the Layout Engine. [ #10107] (ALL prior versions) Applications which use fonts from untrusted ...

[Downloading ICU](#) > [Download ICU 51](#)

### [Ant Setup for Java Developers](#) Oct 9, 2014, 3:59 PM by Yoshito Umaoka

... Build ICU4J API and test classes for running the ICU4J test suite with Java **security** manager enabled secureCheck Run the secure (applet-like) ICU4J test suite stringPrep Modular build of ...

[Setup](#) > [IDE Setup for Java Developers \(ICU4J\)](#) > [Ant Setup for Java Developers](#)

### [Subversion Setup for ICU Developers](#) Apr 20, 2015, 11:25 AM by Andy Heninger

... org. Save the putty configuration. Then click the "open" button. If you get a **security** alert regarding the server's host key not being cached in the registry, respond with ...

[Setup](#) > [Subversion Setup for ICU Developers](#)

### [Download ICU 53](#) Aug 19, 2015, 10:58 AM by Steven R. Loomis

... such as "3 weeks ago" or "next Tuesday." (# 8464) Updated Spoof Checker for Unicode **Security** Standard version 6.3. (# 10706) ICU4C Specific Changes Note: I CU4C now requires compilers with ...

[Downloading ICU](#) > [Download ICU 53](#)

### [Download ICU 54](#) Aug 19, 2015, 10:58 AM by Steven R. Loomis

... release. Known Issues C/J: Spoof Checker not yet updated to Unicode 7.0 **security** data ( #11262) C: In some environments (newer clang, older gcc/libstdc++) ICU may fail to ...

[Downloading ICU](#) > [Download ICU 54](#)

### [Download ICU 49](#) Dec 17, 2012, 12:56 PM by Yoshito Umaoka

... function ( #9218) [ICU4J] ICU4J charset module may trigger NPE on Java 7 when Java **security** manager is enabled. This is a bug in Java 7. ( #9172) ICU4C Download Version: 49



## About

[Home](#)

## Get

[Download](#)

## Contribute

[Start Here](#)

[Report a Bug](#)

[Report a security issue](#)

[Submit a Patch](#)

[Mailing Lists](#)

[Testing QEMU](#)

## Virtualize

[KVM](#)

## Learn

[Documentation](#)

[Links](#)

[License](#)

## Toolbox

[What links here](#)

[Related changes](#)

[Special pages](#)

# SecurityProcess

QEMU takes security very seriously, and we aim to take immediate action to address serious security-related problems that involve our product.

Please report any suspected security vulnerability in QEMU to the following addresses. You can use GPG keys for respective recipients to communicate with us securely. If you do, please upload your GPG public key or supply it to us in some other way, so that we can communicate to you in a secure way, too! Please include the tag [QEMU-SECURITY] on the subject line to help us identify your message as security-related.

QEMU Security Contact List: please copy everyone on this list.

Contact Person(s)	Contact Address	Company	GPG key	GPG key fingerprint
Michael S. Tsirkin	mst@redhat.com	Red Hat Inc.	<a href="#">[GPG key]</a>	Fingerprint=0270 606B 6F3C DF3D 0B17 0970 C350 3912 AFBE 8E67
Petr Matousek	pmatouse@redhat.com	Red Hat Inc.	<a href="#">[GPG key]</a>	Fingerprint=8107 AF16 A416 F9AF 18F3 D874 3E78 6F42 C449 77CA
Stefano Stabellini	stefano.stabellini@eu.citrix.com	Citrix	<a href="#">[GPG key]</a>	Fingerprint=D04E 33AB A51F 67BA 07D3 0AEA 894F 8F48 70E1 AE90
Security Response Team	secalert@redhat.com	Red Hat Inc.	<a href="#">[GPG key]</a>	
Michael Roth	mdroth@linux.vnet.ibm.com	IBM	<a href="#">[GPG key]</a>	Fingerprint=46F5 9FBD 57D6 12E7 BFD4 E2F7 7E15 100C CD36 69B1

## Contents [\[hide\]](#)

- 1 [How to Contact Us Securely](#)
- 2 [How we respond](#)
  - 2.1 [Publication embargo](#)
  - 2.2 [CVE allocation](#)
- 3 [When to Contact the QEMU Security Contact List](#)
- 4 [When not to Contact the QEMU Security Contact List](#)
- 5 [What to Send to the QEMU Security Contact List](#)







Programming with libxml2 is like the thrilling embrace of an exotic strange. It seems to have the potential to fulfil your wildest dreams, but there's a nagging voice somewhere in your head warning you that you're about to get screwed in the worst way.



# Commercial Repositories



isc.org

Blogs

Contact

Donate to ISC

Shop

Customer Login

ISC

Internet Systems Consortium

Software

Support

Community

Network

About Us

Professional Support

ISC Source Code Trees

Public Git Access

Click on one of the links below or navigate to [source.isc.org](#) to access read-only web-based git repositories for BIND and ISC DHCP source code. Navigate to [git.kea.isc.org](#) for the git and bug database for the pre-release Kea project.

BIND

ISC DHCP

Kea

Public releases are always available from the [downloads](#) page on this web site and the [ISC FTP site](#). (When you go to the ISC FTP site, simply select the GUEST option and you will not need a password.) Kea will be posted there beginning with Kea release 1.0, for now it is posted on [kea.isc.org](#).

The BIND and ISC DHCP repositories are mirrors, updated several times per day, of the source repositories maintained by ISC. They contains all the public release branches; upcoming releases can be viewed in their current state at any time. They do *not* contain development branches or unreviewed work in progress. Commits which address security vulnerabilities are withheld until

Developer Menu

> ISC Source Code Trees

> ISC License

> Guidelines for Contributors

> BIND Developer Information

> BIND 9 Coding Style

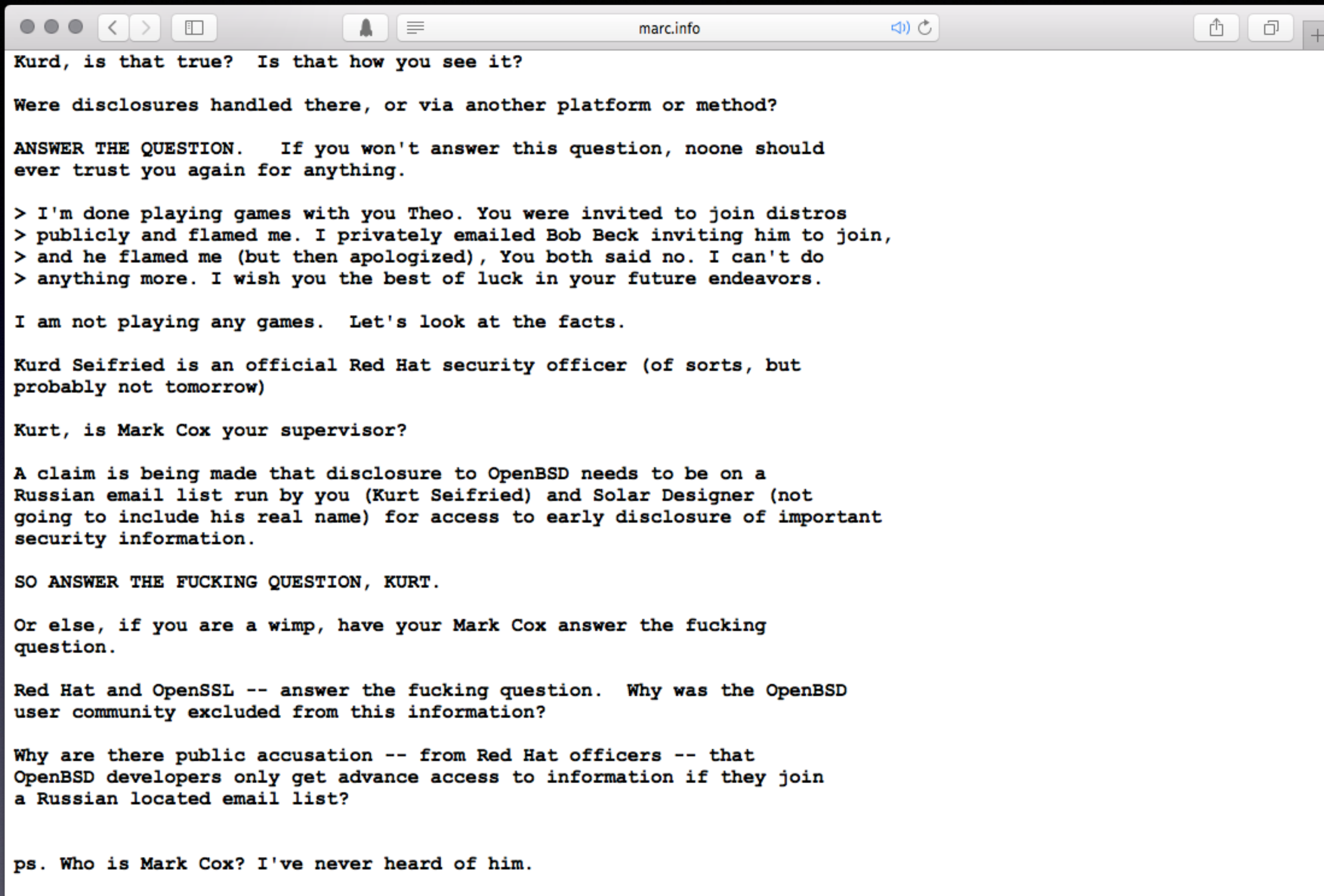
> BIND Contributors Guide

> BIND & DHCP Bug Submission



# OpenSSL





new OpenSSL flaw



## LibreSSL Upstream Patches

When older protocols, algorithms and programming practices are deprecated, often upstream software is not ready for the transition. The OpenBSD project, along with OSes and software distributions, work to patch affected software locally when removals occur, as well as push those changes upstream so that the whole software ecosystem benefits.

The purpose of this page is to track some of the patches maintained in the OpenBSD ports system. The FreeBSD project maintains a related [wiki](#) detailing current issues and porting notes.

### SSLv3

A common mistake is to use `SSLv3_method` or `TLSv1_method` setting up a new `SSL_CTX`. These methods hard-code the connection to a particular protocol version. For example, `TLSv1_method` specifies that only TLS 1.0 should be used, preventing TLS 1.1, 1.2 or later versions. This is almost never what you want.

The more future-proof and secure way is to either use `SSLv23_method` (for compatibility with older versions of LibreSSL/OpenSSL) or the newer `TLS_method`, both of which will negotiate the highest supported protocol. In spite of its name, `SSLv23_method` can actually negotiate a TLS connection with OpenSSL or LibreSSL. As of LibreSSL 2.3.0, `SSLv23_method` only negotiates TLS.

Here are some of the programs and libraries affected by SSLv3 removal. In most cases, support was easily gated with `OPENSSL_NO_SSLV3` checks or by switching to `SSLv23_method`/`TLS_method`. All OpenBSD packages now either have local patches in the ports tree or there is an upstream fix that has not made it into a release yet.

apache-httpd : <a href="#">report</a> , <a href="#">patch</a>	bro : <a href="#">patch</a>	commoncpp : <a href="#">patch</a>
courier-imap : <a href="#">patch</a> <a href="#">patch</a>	e17 : <a href="#">patch</a>	fetchmail : <a href="#">patch</a>
haproxy : <a href="#">patch</a>	httperf : <a href="#">patch</a>	imapfilter : <a href="#">patch</a>
kamailio : <a href="#">patch</a>	luasec : <a href="#">patch</a>	monit : <a href="#">patch</a>
monitoring-plugins : <a href="#">patch</a>	nssl : <a href="#">patch</a>	p5-Crypt-SSLeay : <a href="#">patch</a> <a href="#">patch</a>
p5-Mail-SpamAssassin : <a href="#">patch</a>	php 5.4 : <a href="#">patch</a>	pjsua : <a href="#">patch</a>
py-M2Crypto : <a href="#">patch</a>	qca-openssl : <a href="#">patch</a>	qt4 : <a href="#">patch</a>
ruby 1.8-2.2 : <a href="#">patch</a> <a href="#">patch</a>	socat : <a href="#">patch</a>	squid : <a href="#">patch</a> <a href="#">patch</a>
sslsplit : <a href="#">patch</a>	tn5250 : <a href="#">patch</a>	znc : <a href="#">patch</a>



# Key components & Deadware



# libwmf

CVE-2004-0941

CVE-2007-0455

CVE-2007-2756

CVE-2007-3472

CVE-2007-3473

CVE-2007-3477

CVE-2009-3546

CVE-2015-0848

CVE-2015-4588

CVE-2015-4695

CVE-2015-4696



# Jasper

CVE-2008-3520

CVE-2008-3522

CVE-2011-4516

CVE-2011-4517

CVE-2014-8137

CVE-2014-9029



Widely Deployed



# Wordpress

The patch applied for CVE-2015-5622 in DSA-3332-1 contained a faulty hunk.

This update corrects that problem. For reference, the relevant part of the original advisory text follows.

Several vulnerabilities have been fixed in Wordpress, the popular blogging engine.



PHP



KVM/QEMU/Xen



<http://xenbits.xen.org/xsa/advisory-149.html>

Deployment of the PATCH (or others which are substantially similar) is permitted during the embargo, even on public-facing systems with untrusted guest users and administrators.

However deployment of the (RE)BOOT LIMIT MITIGATION is NOT permitted

(except where all the affected systems and VMs are administered and

used only by organisations which are members of the Xen Project

Security Issues Predisclosure List). Specifically, deployment on public cloud systems is NOT permitted.

This is because applying domain creation and reboot limits in connection with a security issue would be a user-visible change which

could lead to the rediscovery of the vulnerability.



# Co-ordinating with Upstream



“Hacking Team, the GPL-violating Italian company who sells surveillance software to human rights abusers” - Matthew Garrett

Why improving kernel security is important



stunnel



ports/patch-tls.c at master · Sp1l

< > ↺ ⌵

GitHub, Inc. [US] | github.com/Sp1l/ports/blob/master/security/tlswrap/files/patch-tls.c

❤️ 👤

GitHub

This repository Search

Explore Features Enterprise Pricing

Sign up

📁

Sp1l / ports

👁 Watch 1

★ Star 1

🍴 Fork

Branch: master ▾

ports / security / tlswrap / files / patch-tls.c

⋮

🔄 Bernard Spil Proper fix security/tlswrap LibreSSL build

ea87966 on Mar 21

0 contributors

16 lines (15 sloc) | 478 Bytes

Raw Blame History

🖨 ✎ 🗑

```
1 --- tls.c.orig 2015-03-21 13:23:17 UTC
2 +++ tls.c
3 @@ -73,10 +73,12 @@ void tls_init(char *egd_sock) {
4         printf("egd_sock is %s\n", egd_sock);
5         #ifdef HAVE_RANDOM_STATUS
6             if (RAND_status() != 1) {
7 +#ifdef HAVE_RANDOM_EGD
8                 if ( RAND_egd(egd_sock) == -1 ) {
9                     fprintf(stderr, "egd_sock is %s\n", egd_sock);
10                    sys_err("RAND_egd failed\n");
11                }
12 +#endif
13                 if (RAND_status() != 1)
14                     sys_err("ssl_init: System without /dev/urandom, PRNG seeding must be done manually.\r\n");
15             }
```





## Re: Libressl with stunnel

jungle Boogie wrote:

> On 28 March 2015 at 16:54, jungle Boogie <jungleboogie0 <at> gmail.com>

> wrote:

>>

>> Have the developers considered this patch:

>> <https://github.com/sabotage-linux/sabotage/commit/9b47cbbf3ce903dee042c45c8197db066e8e0053>

>

>>

>

> Here's a patch for tlswrap with RAND\_edg:

> <https://github.com/Sp11/ports/blob/master/security/tlswrap/files/patch-tls.c>

The

>

GPL 2.0 section 3 allows stunnel to be linked against

GPL-incompatible libraries included with the operating system.

This is the case for LibreSSL on the FreeBSD operating system.

Nevertheless, I don't support LibreSSL nor extend the OpenSSL GPL exception to allow distributing stunnel linked against LibreSSL for other operating systems.

Mike





**Sevan Janiyan**

@sevanjaniyan

GPL vs an improvement in security posture  
of software, which ultimately helps the actual  
freedom of the user

[comments.gmane.org/gmane.network....](https://comments.gmane.org/gmane.network....)

6:27 PM - 1 Sep 2015







**Michał Trojnara** @mtrojnar · Sep 5

@sevanjaniyan Honestly, I doubt LibreSSL is currently (i.e., after a major code cleanup of both) any more secure than OpenSSL.



1



[View other replies](#)





**Michał Trojnara** @mtrojnar · Oct 18

[@sevanjaniyan](#) I think the recent [#LibreSSL](#) vulnerabilities have just proven me right.



[View other replies](#)





**Michał Trojnara** ฅ  
@mtrojnara

You are blocked from following @mtrojnara and viewing @mtrojnara's Tweets. [Learn more](#)



musl libc / Alpine Linux



GCC / Binutils