Predicting Vulnerable Software Components

Stephan Neuhaus

Thomas Zimmermann
Andreas Zeller

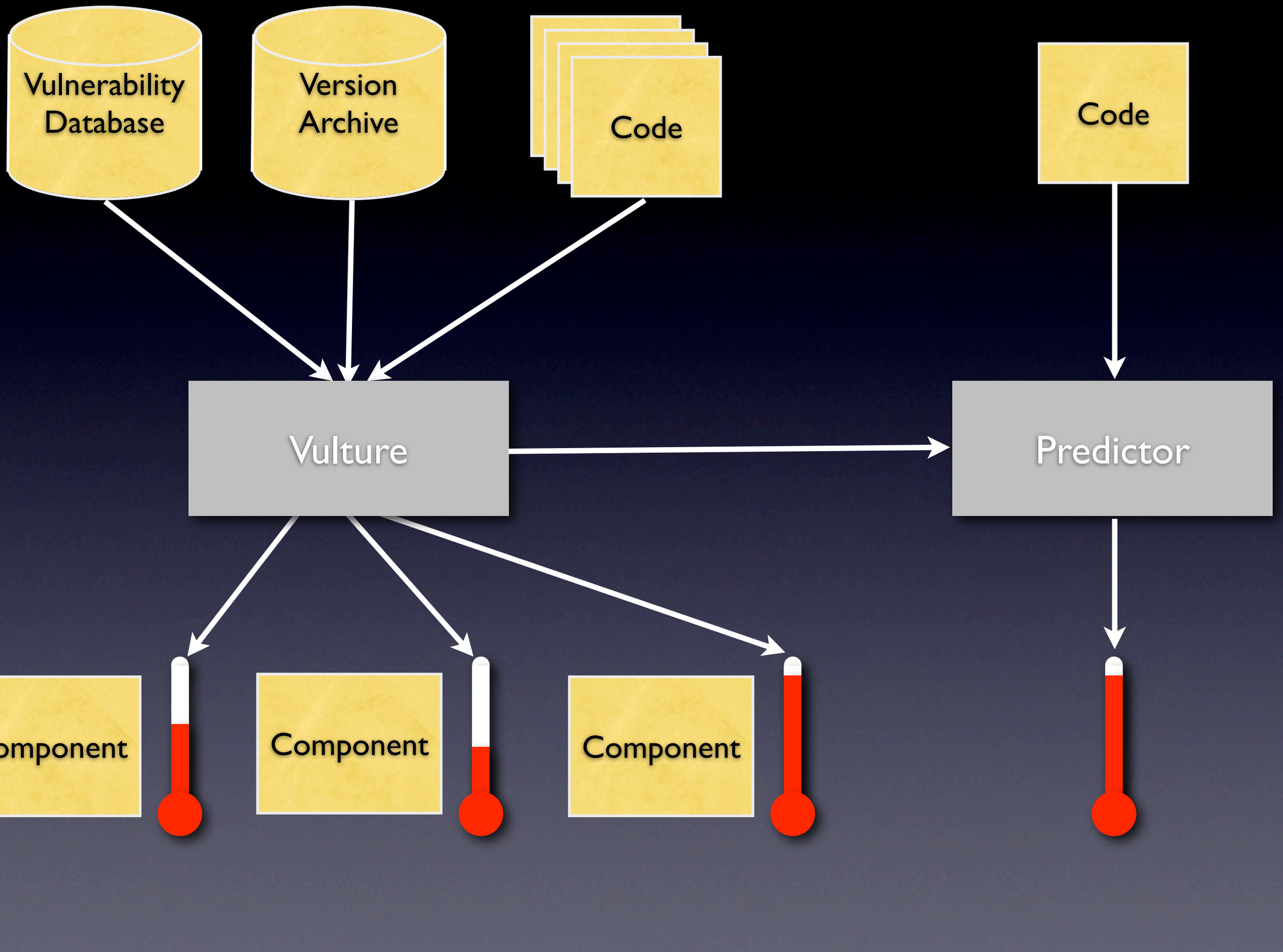
Security Advisory 2006-76

Title: XSS using outer windows Function object
Impact: High
Products: Firefox 2.0
Description: moz_bug_r_a4 demonstrated that the Function prototype regression described in bug 355161 could be exploited to bypass the protections against cross site script (XSS) injection, which could be used to steal credentials or sensitive data from arbitrary sites or perform destructive actions on behalf of a logged-in user.

Is this new component likely to be vulnerable?

What other components are vulnerable?

0 → Vulnerabilities


Vulnerability Database
Version Archive
Code
Code
Vulture
Predictor
Component
Component
Component

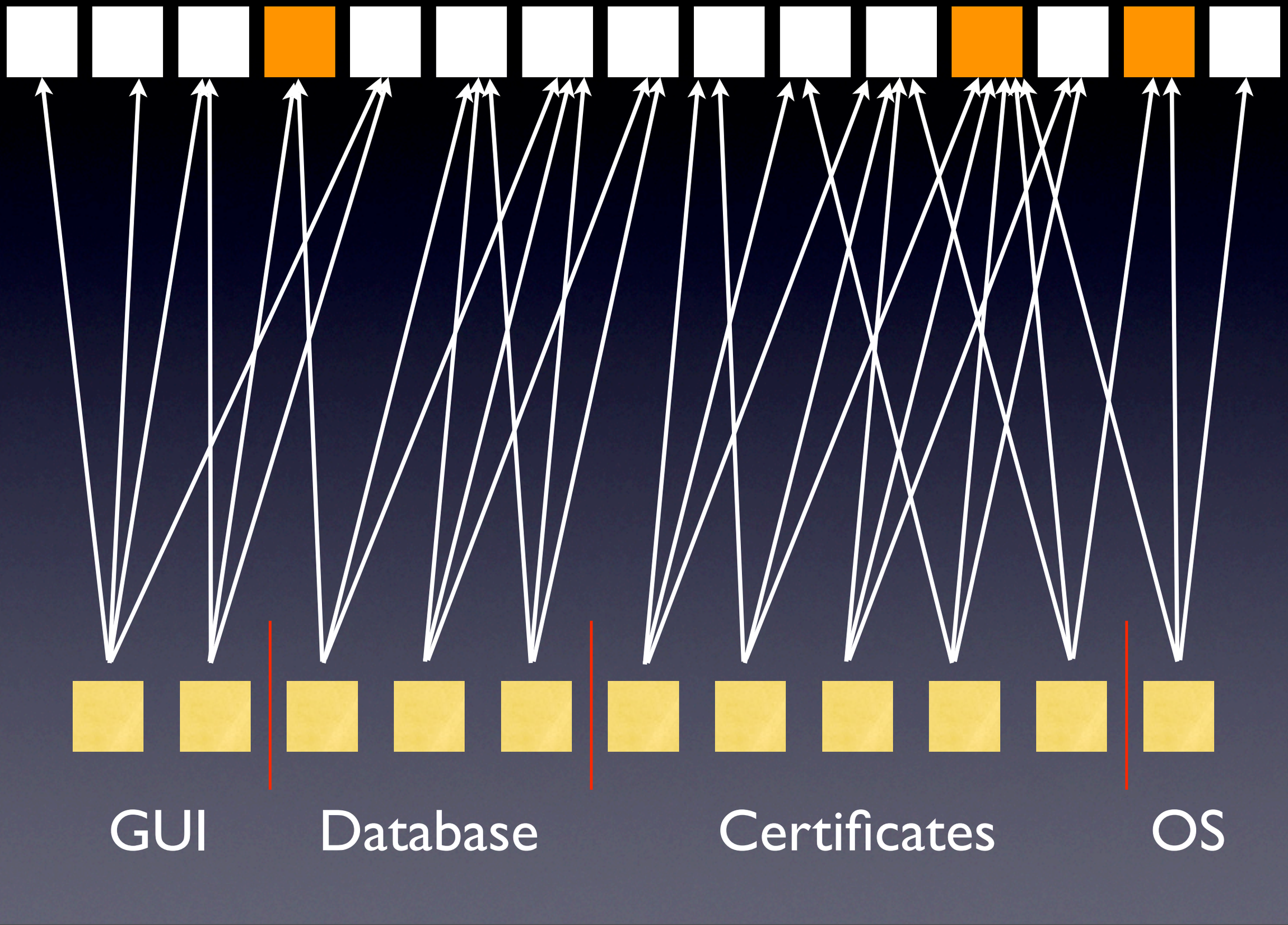
Programmer

Code Complexity

Look for features that are *invariant* under evolution

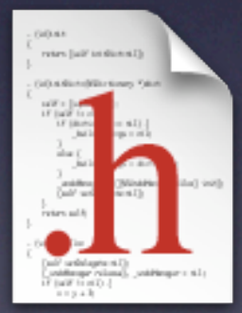
Language

Imports

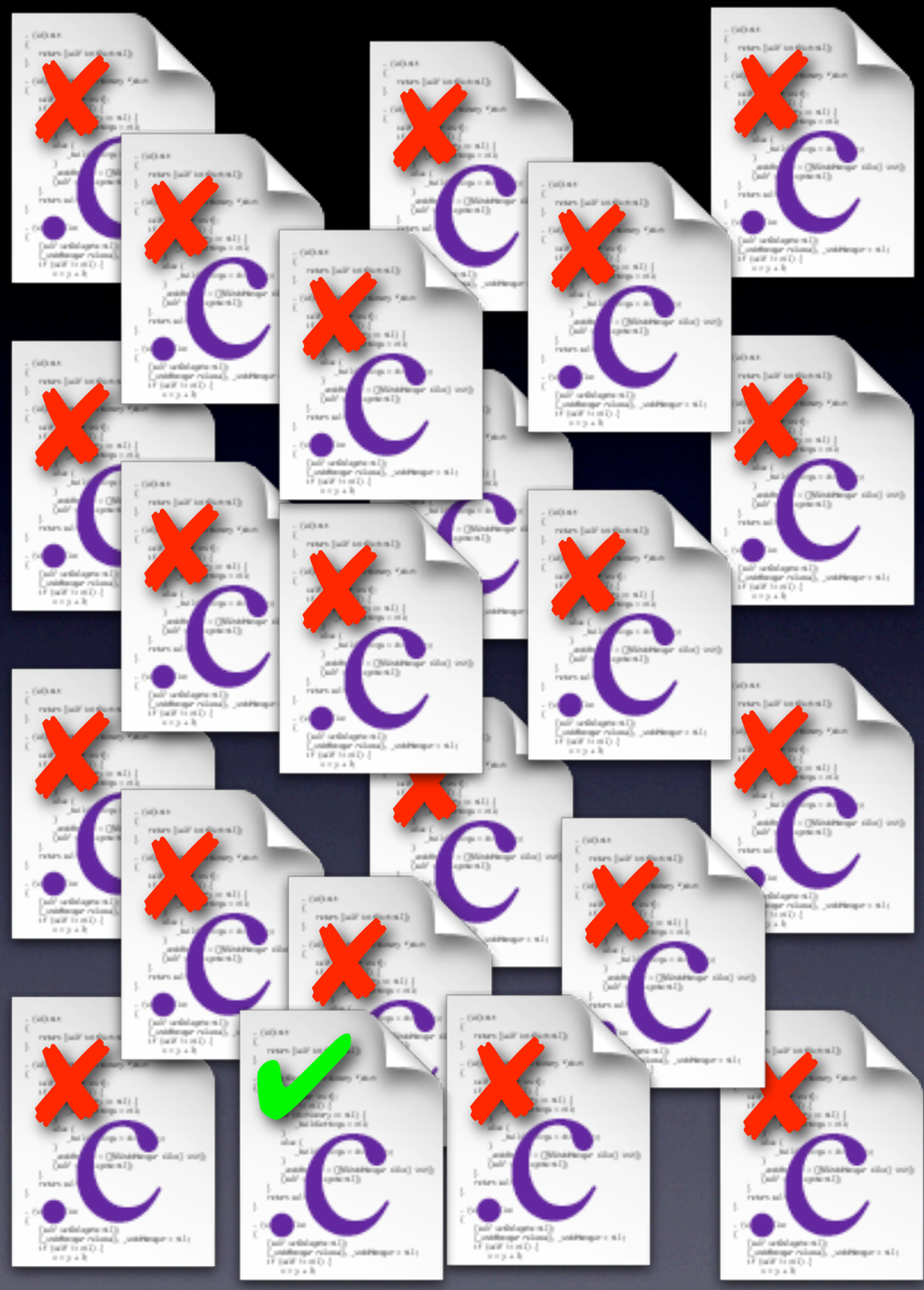


nsIContent.h

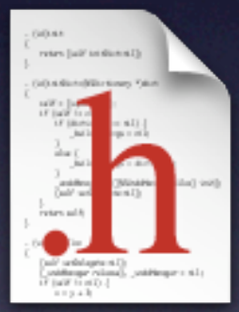
nsIContentUtils.h



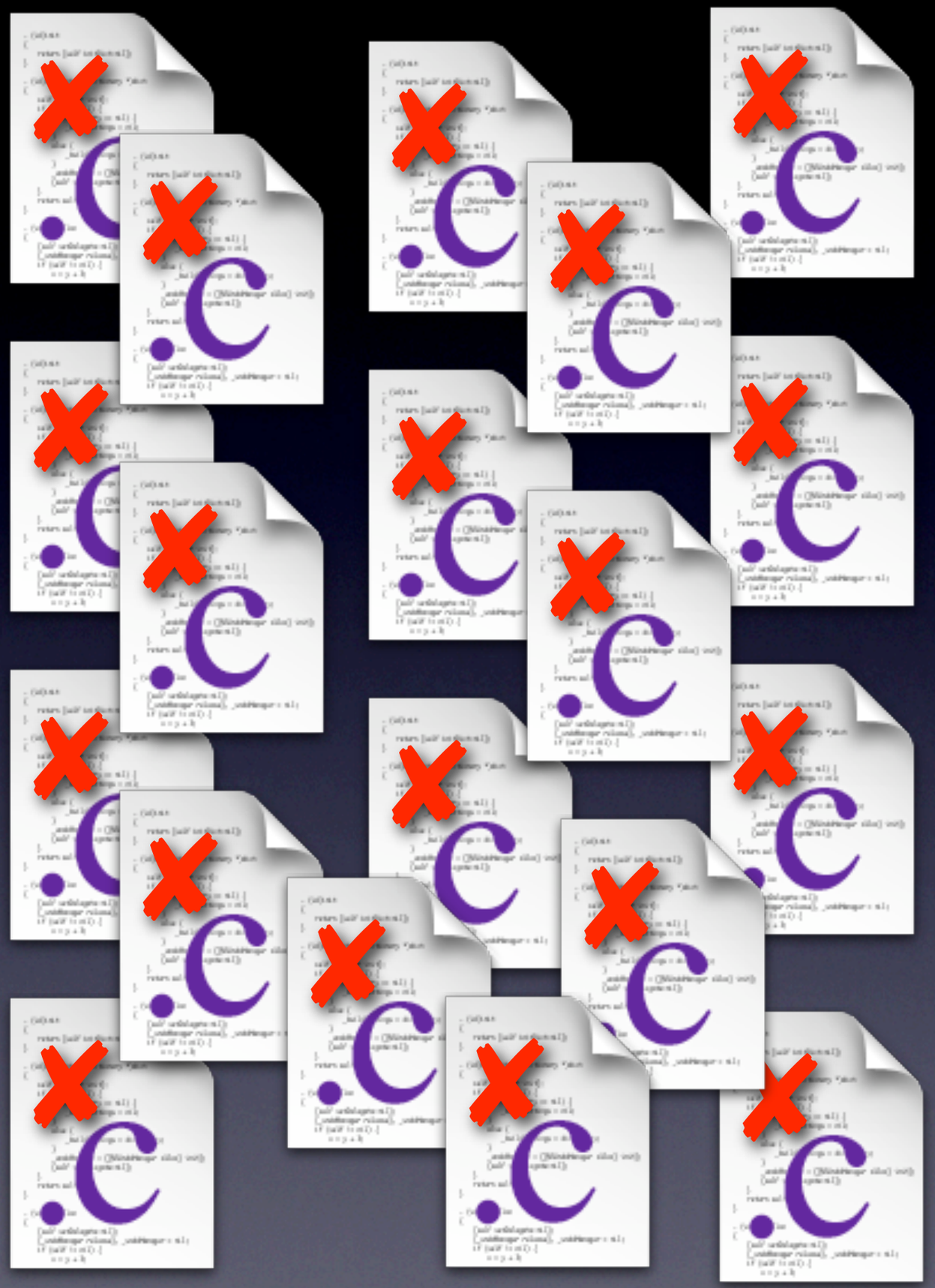
nsIScriptSecurityManager.h



nsIPrivateDOMEvent.h



nsReadableUtils.h



Research Questions

- How well do imports predict vulnerabilities?
- Can imports be used for classification (vulnerable or not) and for regression (number of vulnerabilities)?

Case Study: Mozilla

- CVS from January 4, 2007
- 14,368 C/C++ files
- 134 Security Advisories since January 2005
- Only 424 vulnerable components (4.05%)

⇒ *Prediction is challenging*

MFSA 2006-74: Mail header processing heap overflows

http://www.mozilla.org/security/announce/2006/mfsa2006-74.html

Getting Started Latest Headlines

mozilla.org

search mozilla: Go

Products Support Store Developers About

- Roadmap
- Projects
- Coding
  - Module Owners
  - Hacking
  - Get the Source
  - Build It
- Testing
  - Releases
  - Nightly Builds
  - Report A Problem
- Tools
  - Bugzilla
  - Tinderbox
  - Bonsai
  - LXR
- FAQs

Mozilla Foundation Security Advisory 2006-74

Title: Mail header processing heap overflows
Impact: Critical
Announced: December 19, 2006
Reporter: Georgi Guninski, David Bienvenu
Products: Thunderbird, SeaMonkey

Fixed in: Thunderbird 1.5.0.9
SeaMonkey 1.0.7

Description

Georgi Guninski reported that long Content-Type headers in external message bodies could cause a heap buffer overflow when processing mail headers. While working on that code David Bienvenu discovered a similar overflow could occur when processing long rfc2047-encoded headers.

Either overflow could be exploited to execute arbitrary code.

Workaround

None, upgrade to a fixed

References

https://bugzilla.mozilla.c
https://bugzilla.mozilla.c
CVE-2006-6505

gi?id=362213
gi?id=362512

Portions of this content are © 1998–2

Last modified

Find: 2006-74

Done

CVS Log for mimeebod.cpp (1.27)

http://bonsai.mozilla.org/cvslog.cgi?file=mozilla%2Fmailnews%2Fmime%2Fsrc%

mozilla cvs

Getting Started Latest Headlines

CVS

mozilla

Rev A

1.27 bi
1.26 jo
1.25 ti
1.24 ge
1.23 ge
1.22 ca
1.21 ti
1.20 ca
1.19 ca
1.18 ge
1.17 ti
1.16 jg
1.14 w
1.13 rh
1.12 ric
1.11 al

CVS Log for comi18n.cpp (1.125)

http://bonsai.mozilla.org/cvslog.cgi?file=mozilla%2Fmailnews%2Fmime%2Fsrc%

keynote mask with shape

Getting Started Latest Headlines

mozilla.org

Bonsai version 1.3.9

lxr Browse the source code as hypertext.
diff Compare any two version.
blame Annotate the author of each line.
RSS Get an RSS version of this page.
graph View the revision history as a graph

CVS Log

mozilla/ mailnews/ mime/ src/ comi18

Log
fix 362512 issues
Bug 147697: asso

Rev	Author	Date	
1.125	bienvenu%nventure.com	2006-1	sr=mscott
1.124	smontagu%smontagu.org	2006-1	mail: generate_encodedwords(), output_carryoverlen
1.123	cbiesinger%web.de	2006-0	replacing them with *UTF16* ones
1.122	db48x%yahoo.com	2005-01-15 02:32	bug 226205: MailNews should use the newer nsIPrefService APIs instead of nsIPref patch by Mikael Parknert <mikael@parknert.se>, r=niel, sr=darin
1.121	darin%meer.net	2004-11-01 10:50	eliminating uses of deprecated nsComponentManager:: methods (bug 267040), r=bsmedberg
1.120	scott%scott-macgregor.org	2004-05-07 11:13	Bug #242065 - "My Name" from account is ignored when email contains "special chars", full name extracted from email address Patch by ch.ey@gmx.net sr=mscott
1.119	gerv%gerv.net	2004-04-17 11:33	Bug 236613: change to MPL/LGPL/GPL tri-license.
1.118	darin%meer.net	2004-02-19 17:53	landing patch for bug 234864 "string branch landing resulted in large spike in heap allocations (bmd:A metric)" r+sr=dbaron this patch also introduces nsTFixedString and removes CBufDescriptor.
1.117	jshin%mailaps.org	2003-06-12 14:57	bug 167265 : add to necko Content-Disposition header handling per RFC 2231 (with fallbacks to RFC 2047 and raw 8bit chars in leOriginCharset!) necessary for
1.116	alecf%flett.org		
1.115	alecf%netscape.com		
1.114	alecf%netscape.com		
1.113	alecf%netscape.com		

Find: mask

Done

Aquamacs – mimeebod.h

```
 * use your version
 * decision by delet
 * and other provisi
 * the provisions ab
 * the terms of any
 *
 * ***** END LICENSE

#ifndef _MIMEEBOD_H_
#define _MIMEEBOD_H_

#include "mimeobj.h"

/* The MimeExternalB
   (This is not to b
   handler for appli
   handlers.)
 */

typedef struct MimeE
typedef struct MimeE

struct MimeExternalB
  MimeObjectClass ob
};

extern MimeExternalB

struct MimeExternalB
  MimeObject object;
  MimeHeaders *hdrs;

  char *body;
};

#endif /* _MIMEEBOD_
```

-:-- mimeebod.h
Wrong type argument:

Aquamacs – mimeebod.cpp

```
 * ***** END LICENSE BLOCK ***** */
#include "nsCOMPtr.h"
#include "nsIURL.h"
#include "mimeebod.h"
#include "prmem.h"
#include "nsCRT.h"
#include "plstr.h"
#include "prlog.h"
#include "prio.h"
#include "nsFileSpec.h"
#include "nsEscape.h"
#include "msgCore.h"
#include "nsMimeStringResources.h"
#include "mimemoz2.h"

#define MIME_SUPERCLASS mimeObjectClass
MimeDefClass(MimeExternalBody, MimeExternalBodyClass,
             mimeExternalBodyClass, &MIME_SUPERCLASS);

#ifdef XP_MACOSX
extern MimeObjectClass mimeMultipartAppleDoubleClass;
#endif

static int MimeExternalBody_initialize (MimeObject *);
static void MimeExternalBody_finalize (MimeObject *);
static int MimeExternalBody_parse_line (const char *, PRInt32, MimeObject *);
static int MimeExternalBody_parse_eof (MimeObject *, PRBool);
static PRBool MimeExternalBody_displayable_inline_p (MimeObjectClass *clazz,
                                                     MimeHeaders *hdrs);

#if 0
#if defined(DEBUG) && defined(XP_UNIX)
static int MimeExternalBody_debug_print (MimeObject *, PRFileDesc *, PRInt32);
#endif
#endif /* 0 */

static int
MimeExternalBodyClassInitialize(MimeExternalBodyClass *clazz)
```

-:-- mimeebod.cpp 13% (37,0) (C/l Abbrev Fill)
Undo!

Aquamacs – comi18n.h

```
 * decision by deleti
 * and other provisio
 * the provisions abo
 * the terms of any o
 *
 * ***** END LICENSE
#ifndef _COMI18N_LOAD
#define _COMI18N_LOAD

#include "msgCore.h"

//#ifndef kMIME_ENCOD
//#define kMIME_ENCOD
//#endif

#ifndef kMAX_CSNAME
#define kMAX_CSNAME 6
#endif

class nsIUnicodeDecod
class nsIUnicodeEncod
class nsIStringCharse

#ifdef __cplusplus
extern "C" {
#endif /* __cplusplus

/**
 * Decode MIME header
 * Uses MIME_ConvertC
 *
 *
 * @param header
 * @param default_cha
8 8bit data
 * @param override_ch
ny charset labeling o
```

-:-- comi18n.h
Wrong type argument:

Aquamacs – comi18n.cpp

```
static const char hexdigits[] = "0123456789ABCDEF";

static PRInt32
intlmime_encode_q(const unsigned char *src, PRInt32 srcsize, char *out)
{
  const unsigned char *in = (unsigned char *) src;
  const unsigned char *end = in + srcsize;
  char *head = out;

  for (; in < end; in++) {
    if (NO_Q_ENCODING_NEEDED(*in)) {
      *out++ = *in;
    }
    else if (*in == ' ') {
      *out++ = '_';
    }
    else {
      *out++ = '=';
      *out++ = hexdigits[*in >> 4];
      *out++ = hexdigits[*in & 0xF];
    }
  }
  *out = '\0';
  return (out - head);
}

static void
encodeChunk(const unsigned char* chunk, char* output)
{
  register PRInt32 offset;

  offset = *chunk >> 2;
  *output++ = basis_64[offset];

  offset = ((*chunk << 4) & 0x30) + (*(chunk+1) >> 4);
  *output++ = basis_64[offset];
```

-:-- comi18n.cpp 13% (80,0) (C++/l Abbrev Fill)

MFSA 2006-74: Mail header processing heap overflows

http://www.mozilla.org/security/announce/2006/mfsa2006-74.html

Getting Started Latest Headlines

mozilla.org

search mozilla: Go

Products Support Store Developers About

- Roadmap
- Projects
- Coding
  - Module Owners
  - Hacking
  - Get the Source
  - Build It
- Testing
  - Releases
  - Nightly Builds
  - Report A Problem
- Tools
  - Bugzilla
  - Tinderbox
  - Bonsai
  - LXR
- FAQs

Mozilla Foundation Security Advisory 2006-74

Title: Mail header processing heap overflows
Impact: Critical
Announced: December 19, 2006
Reporter: Georgi Guninski, David Bienvenu
Products: Thunderbird, SeaMonkey

Fixed in: Thunderbird 1.5.0.9
SeaMonkey 1.0.7

Description

Georgi Guninski reported that long Content-Type headers in external message bodies could cause a heap buffer overflow when processing mail headers. While working on that code David Bienvenu discovered a similar overflow could occur when processing long rfc2047-encoded headers.

Either overflow could be exploited to execute arbitrary code.

Workaround

None, upgrade to a fixed version immediately.

References

https://bugzilla.mozilla.org/show_bug.cgi?id=362213
https://bugzilla.mozilla.org/show_bug.cgi?id=362512
CVE-2006-6505

Portions of this content are © 1998–

Last modifie

Find: 2006-74

Done

CVS Log for mimeebod.cpp (1.27)

http://bonsai.mozilla.org/cvslog.cgi?file=mozilla%2Fmailnews%2Fmime%2Fsrc%

Getting Started Latest Headlines

mozilla cvs

CVS Log for comi18n.cpp (1.125)

keynote mask with shape

mozilla.org

Bonsai version 1.3.9

CVS Log

mozilla/ mailnews/ mime/ src/ mimeebod.cpp (1.27)

lxr Browse the source code as hypertext.
diff Compare any two version.
blame Annotate the author of each line.
RSS Get an RSS version of this page.
graph View the revision history as a graph

CVS Log

mozilla/ mailnews/ mime/ src/ comi18n.cpp (1.125)

lxr Browse the source code as hypertext.
diff Compare any two version.
blame Annotate the author of each line.
RSS Get an RSS version of this page.
graph View the revision history as a graph

Rev	Author	Date	Log
1.125	bienvenu%nventure.com	2006-12-01 11:24	fix 362512 issues with rfc2047 encoding, sr=mscott
1.124	smontagu%smontagu.org	2006-10-18 00:49	Bug 147697: assertion every time I send mail: generate_encodedwords(), output_carryoverlen must be > 0, r=ducarroz, sr=bienvenu
1.123	cbiesinger%web.de	2006-02-03 06:18	bug 183156 remove *UCS2* functions, replacing them with *UTF16* ones r+sr=darin
1.122	db48x%yahoo.com	2005-01-15 02:32	bug 226005: MailNews should use the newer nsIPrefService APIs instead of nsIPref patch by Mikael Parknert <mikael@parknert.se>, r=niel, sr=darin
1.121	darin%meer.net	2004-11-01 10:50	eliminating uses of deprecated nsComponentManager:: methods (bug 267040), r=bsmedberg
1.120	scott%scott-macgregor.org	2004-05-07 11:13	Bug #242065 --> "My Name" from account is ignored when email contains "special chars", full name extracted from email address Patch by ch.ey@gmx.net sr=mscott
1.119	gerv%gerv.net	2004-04-17 11:33	Bug 236613: change to MPL/LGPL/GPL tri-license.
1.118	darin%meer.net	2004-02-19 17:53	landing patch for bug 234864 "string branch landing resulted in large spike in heap allocations (brad:A metric)" r+sr=dbaron
1.117	jshin%mailaps.org	2003-06-12 14:57	this patch also introduces nsTFixedString and removes CBufDescriptor. bug 167265 : add to necko Content-Disposition header handling per RFC 2231 (with
1.116	alecf%flett.org	1999-11-05	
1.115	alecf%netscape.com	1999-10-13	
1.114	alecf%netscape.com	1999-10-06	
1.113	alecf%netscape.com	1999-09-04	
1.112	alecf%netscape.com	1999-06-15	
1.111	alecf%netscape.com	1999-05-28	
1.110	alecf%netscape.com	1999-05-04	
1.109	alecf%netscape.com	1999-04-12	
1.108	alecf%netscape.com	1999-03-13	
1.107	alecf%netscape.com	1999-02-12	
1.106	alecf%netscape.com	1999-01-29	
1.105	alecf%netscape.com	1999-01-15	
1.104	alecf%netscape.com	1998-12-04	
1.103	alecf%netscape.com	1998-11-19	
1.102	alecf%netscape.com	1998-11-13	
1.101	alecf%netscape.com	1998-11-12	
1.100	alecf%netscape.com	1998-11-12	
1.99	alecf%netscape.com	1998-11-12	
1.98	alecf%netscape.com	1998-11-12	
1.97	alecf%netscape.com	1998-11-12	
1.96	alecf%netscape.com	1998-11-12	
1.95	alecf%netscape.com	1998-11-12	
1.94	alecf%netscape.com	1998-11-12	
1.93	alecf%netscape.com	1998-11-12	
1.92	alecf%netscape.com	1998-11-12	
1.91	alecf%netscape.com	1998-11-12	
1.90	alecf%netscape.com	1998-11-12	
1.89	alecf%netscape.com	1998-11-12	
1.88	alecf%netscape.com	1998-11-12	
1.87	alecf%netscape.com	1998-11-12	
1.86	alecf%netscape.com	1998-11-12	
1.85	alecf%netscape.com	1998-11-12	
1.84	alecf%netscape.com	1998-11-12	
1.83	alecf%netscape.com	1998-11-12	
1.82	alecf%netscape.com	1998-11-12	
1.81	alecf%netscape.com	1998-11-12	
1.80	alecf%netscape.com	1998-11-12	
1.79	alecf%netscape.com	1998-11-12	
1.78	alecf%netscape.com	1998-11-12	
1.77	alecf%netscape.com	1998-11-12	
1.76	alecf%netscape.com	1998-11-12	
1.75	alecf%netscape.com	1998-11-12	
1.74	alecf%netscape.com	1998-11-12	
1.73	alecf%netscape.com	1998-11-12	
1.72	alecf%netscape.com	1998-11-12	
1.71	alecf%netscape.com	1998-11-12	
1.70	alecf%netscape.com	1998-11-12	
1.69	alecf%netscape.com	1998-11-12	
1.68	alecf%netscape.com	1998-11-12	
1.67	alecf%netscape.com	1998-11-12	
1.66	alecf%netscape.com	1998-11-12	
1.65	alecf%netscape.com	1998-11-12	
1.64	alecf%netscape.com	1998-11-12	
1.63	alecf%netscape.com	1998-11-12	
1.62	alecf%netscape.com	1998-11-12	
1.61	alecf%netscape.com	1998-11-12	
1.60	alecf%netscape.com	1998-11-12	
1.59	alecf%netscape.com	1998-11-12	
1.58	alecf%netscape.com	1998-11-12	
1.57	alecf%netscape.com	1998-11-12	
1.56	alecf%netscape.com	1998-11-12	
1.55	alecf%netscape.com	1998-11-12	
1.54	alecf%netscape.com	1998-11-12	
1.53	alecf%netscape.com	1998-11-12	
1.52	alecf%netscape.com	1998-11-12	
1.51	alecf%netscape.com	1998-11-12	
1.50	alecf%netscape.com	1998-11-12	
1.49	alecf%netscape.com	1998-11-12	
1.48	alecf%netscape.com	1998-11-12	
1.47	alecf%netscape.com	1998-11-12	
1.46	alecf%netscape.com	1998-11-12	
1.45	alecf%netscape.com	1998-11-12	
1.44	alecf%netscape.com	1998-11-12	
1.43	alecf%netscape.com	1998-11-12	
1.42	alecf%netscape.com	1998-11-12	
1.41	alecf%netscape.com	1998-11-12	
1.40	alecf%netscape.com	1998-11-12	
1.39	alecf%netscape.com	1998-11-12	
1.38	alecf%netscape.com	1998-11-12	
1.37	alecf%netscape.com	1998-11-12	
1.36	alecf%netscape.com	1998-11-12	
1.35	alecf%netscape.com	1998-11-12	
1.34	alecf%netscape.com	1998-11-12	
1.33	alecf%netscape.com	1998-11-12	
1.32	alecf%netscape.com	1998-11-12	
1.31	alecf%netscape.com	1998-11-12	
1.30	alecf%netscape.com	1998-11-12	
1.29	alecf%netscape.com	1998-11-12	
1.28	alecf%netscape.com	1998-11-12	
1.27	alecf%netscape.com	1998-11-12	
1.26	alecf%netscape.com	1998-11-12	
1.25	alecf%netscape.com	1998-11-12	
1.24	alecf%netscape.com	1998-11-12	
1.23	alecf%netscape.com	1998-11-12	
1.22	alecf%netscape.com	1998-11-12	
1.21	alecf%netscape.com	1998-11-12	
1.20	alecf%netscape.com	1998-11-12	
1.19	alecf%netscape.com	1998-11-12	
1.18	alecf%netscape.com	1998-11-12	
1.17	alecf%netscape.com	1998-11-12	
1.16	alecf%netscape.com	1998-11-12	
1.15	alecf%netscape.com	1998-11-12	
1.14	alecf%netscape.com	1998-11-12	
1.13	alecf%netscape.com	1998-11-12	
1.12	alecf%netscape.com	1998-11-12	
1.11	alecf%netscape.com	1998-11-12	

Find: mask

Done

Aquamacs – mimeebod.h

```
* use your version
* decision by delet
* and other provisi
* the provisions ab
* the terms of any
*
* ***** END LICENSE

#ifndef _MIMEEBOD_H_
#define _MIMEEBOD_H_

#include "mimeobj.h"

/* The MimeExternalB
   (This is not to b
   handler for appli
   handlers.)
 */

typedef struct MimeE
typedef struct MimeE

struct MimeExternalB
  MimeObjectClass ob
};

extern MimeExternalB

struct MimeExternalB
  MimeObject object;
  MimeHeaders *hdrs;

  char *body;
};

#endif /* _MIMEEBOD_
```

-:-- **mimeebod.h**
Wrong type argument:

Aquamacs – mimeebod.cpp

```
 * ***** END LICENSE BLOCK ***** */
#include "nsCOMPtr.h"
#include "nsIURL.h"
#include "mimeebod.h"
#include "prmem.h"
#include "nsCRT.h"
#include "plstr.h"
#include "prlog.h"
#include "prio.h"
#include "nsFileSpec.h"
#include "nsEscape.h"
#include "msgCore.h"
#include "nsMimeStringResources.h"
#include "mimemoz2.h"

#define MIME_SUPERCLASS mimeObjectClass
MimeDefClass(MimeExternalBody, MimeExternalBodyClass,
             mimeExternalBodyClass, &MIME_SUPERCLASS);

#ifdef XP_MACOSX
extern MimeObjectClass mimeMultipartAppleDoubleClass;
#endif

static int MimeExternalBody_initialize (MimeObject *);
static void MimeExternalBody_finalize (MimeObject *);
static int MimeExternalBody_parse_line (const char *, PRInt32, MimeObject *);
static int MimeExternalBody_parse_eof (MimeObject *, PRBool);
static PRBool MimeExternalBody_displayable_inline_p (MimeObjectClass *clazz,
                                                     MimeHeaders *hdrs);

#if 0
#if defined(DEBUG) && defined(XP_UNIX)
static int MimeExternalBody_debug_print (MimeObject *, PRFileDesc *, PRInt32);
#endif
#endif /* 0 */

static int
MimeExternalBodyClassInitialize(MimeExternalBodyClass *clazz)
```

-:-- **mimeebod.cpp** 13% (37,0) (C/l Abbrev Fill)
Undo!

Aquamacs – comi18n.h

```
 * decision by deleti
 * and other provisio
 * the provisions abo
 * the terms of any o
 *
 * ***** END LICENSE
#ifndef _COMI18N_LOAD
#define _COMI18N_LOAD

#include "msgCore.h"

//#ifndef kMIME_ENCOD
//#define kMIME_ENCOD
//#endif

#ifndef kMAX_CSNAME
#define kMAX_CSNAME 6

class nsIUnicodeDecod
class nsIUnicodeEncod
class nsIStringCharse

#ifdef __cplusplus
extern "C" {
#endif /* __cplusplus

/**
 * Decode MIME header
 * Uses MIME_ConvertC
 *
 *
 * @param header
 * @param default_cha
 * 8bit data
 * @param override_ch
 * charset labeling o
```

-:-- **comi18n.h**
Wrong type argument:

Aquamacs – comi18n.cpp

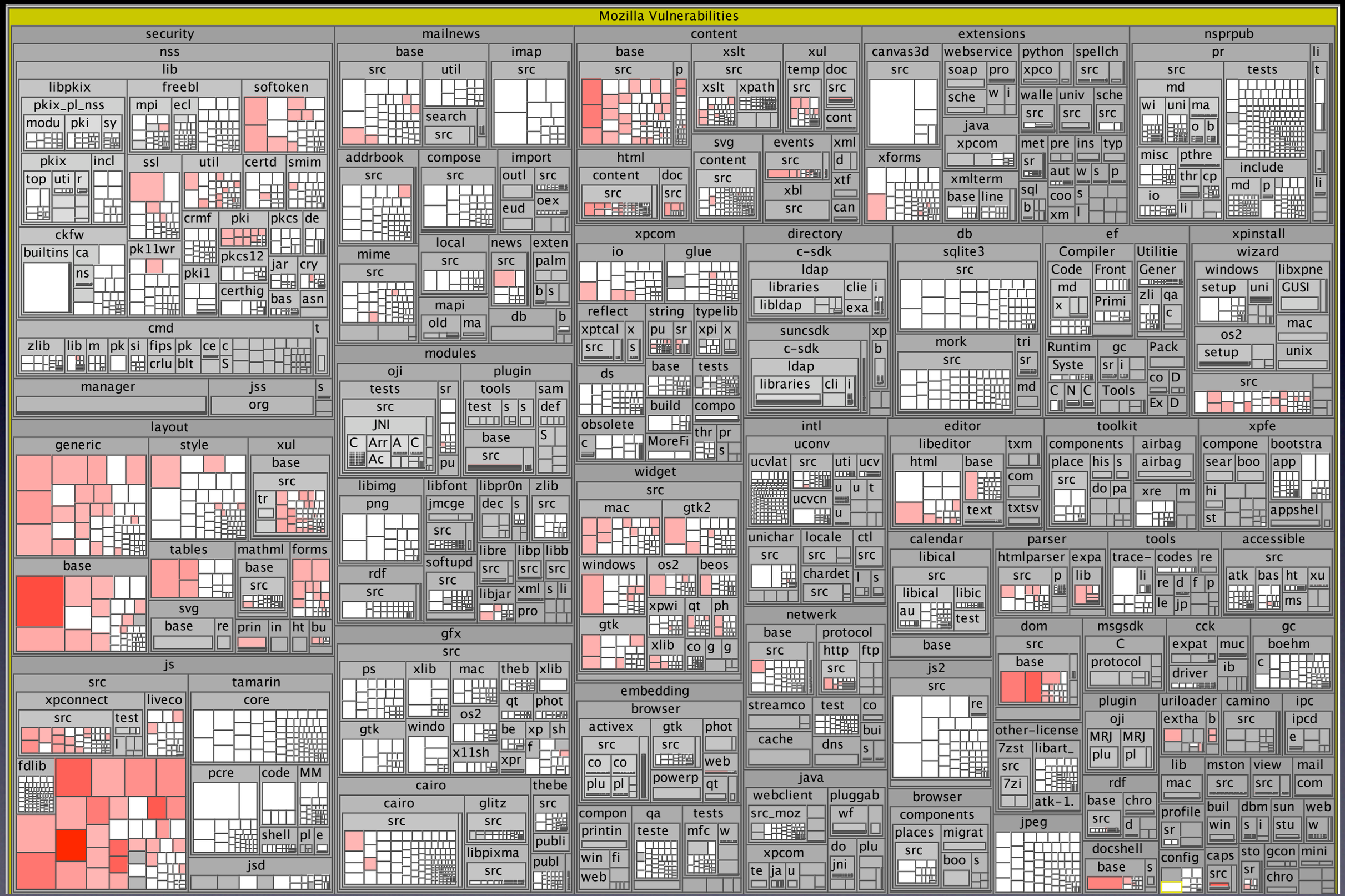
```
static const char hexdigits[] = "0123456789ABCDEF";

static PRInt32
intlmime_encode_q(const unsigned char *src, PRInt32 srcsize, char *out)
{
  const unsigned char *in = (unsigned char *) src;
  const unsigned char *end = in + srcsize;
  char *head = out;

  for (; in < end; in++) {
    if (NO_Q_ENCODING_NEEDED(*in)) {
      *out++ = *in;
    }
    else if (*in == ' ') {
      *out++ = '_';
    }
    else {
      *out++ = '=';
      *out++ = hexdigits[*in >> 4];
      *out++ = hexdigits[*in & 0xF];
    }
  }
  *out = '\0';
  return (out - head);
}

static void
encodeChunk(const unsigned char* chunk, char* output)
{
  register PRInt32 offset;

  offset = *chunk >> 2;
  *output++ = basis_64[offset];

  offset = ((*chunk << 4) & 0x30) + (*(chunk+1) >> 4);
  *output++ = basis_64[offset];
```

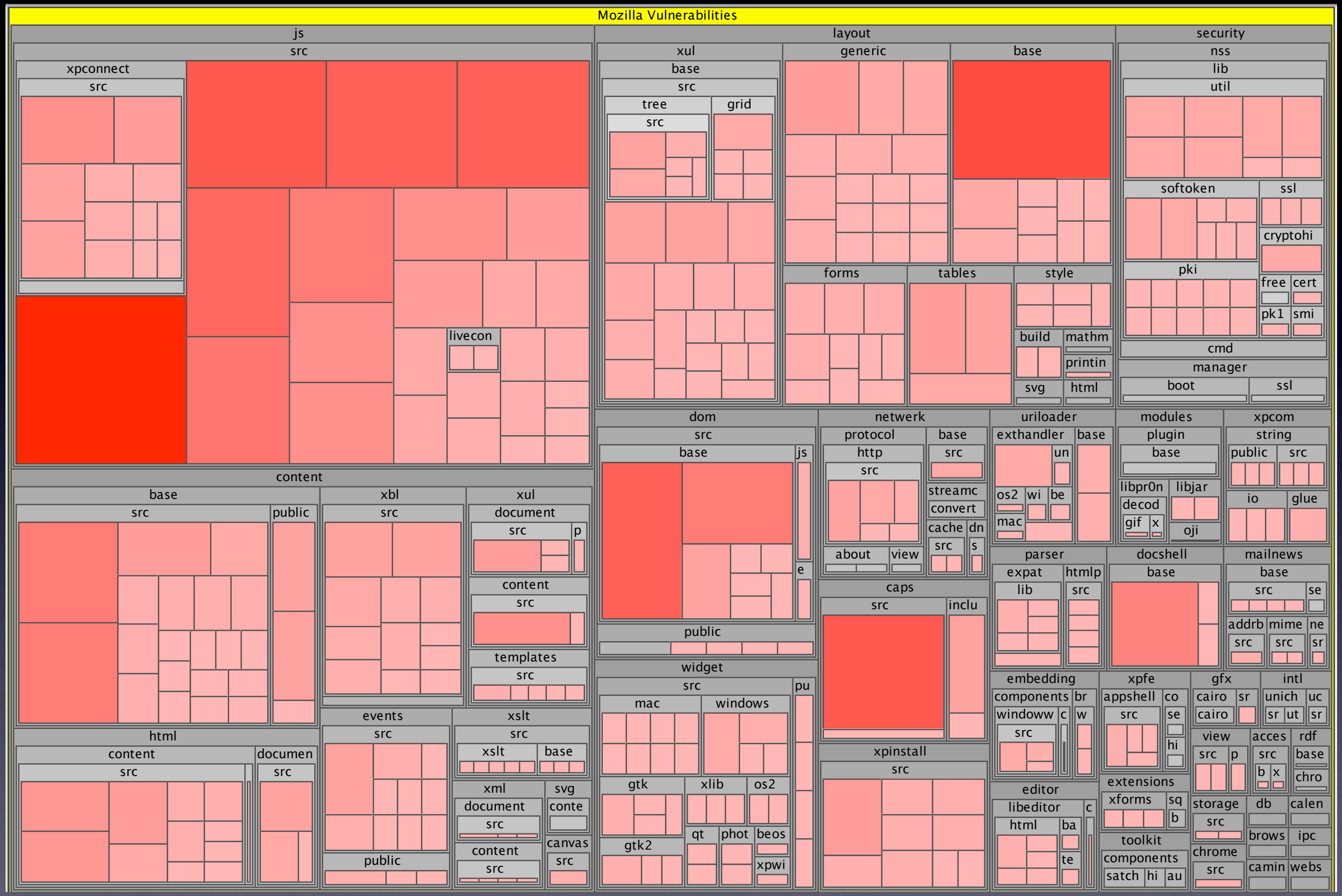
-:-- **comi18n.cpp** 13% (80,0) (C++/l Abbrev Fill)

10,452 components in Mozilla

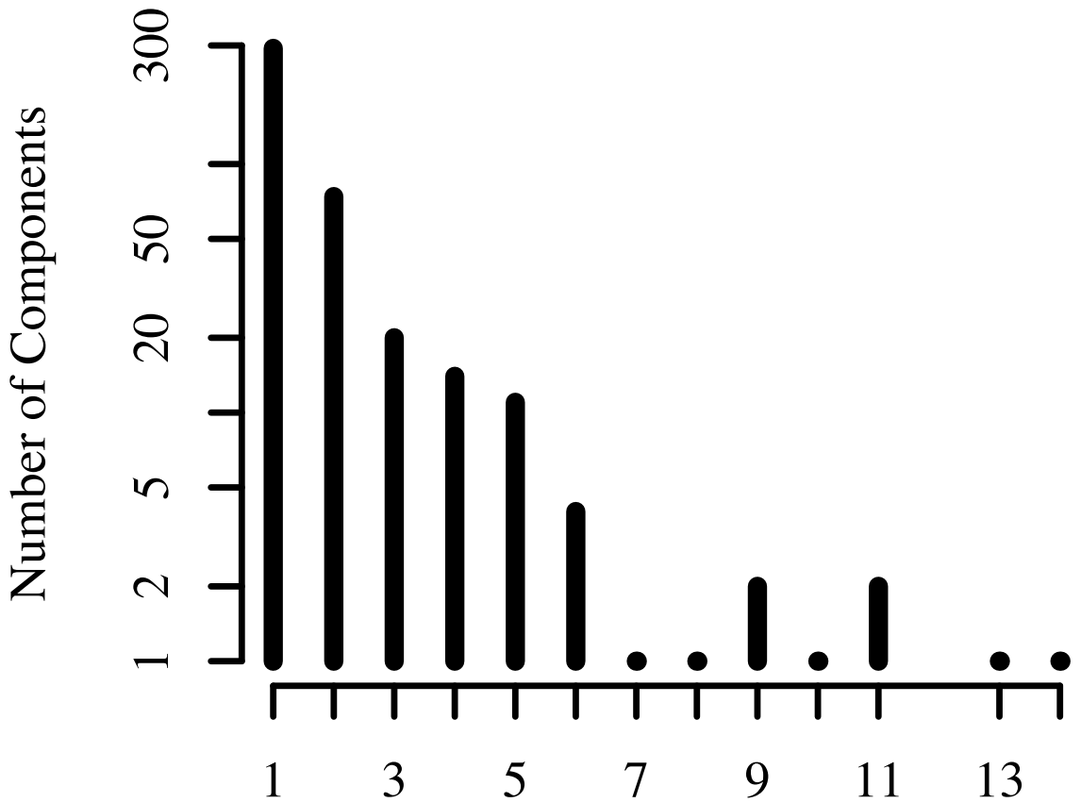
424 vulnerable components

4.05%

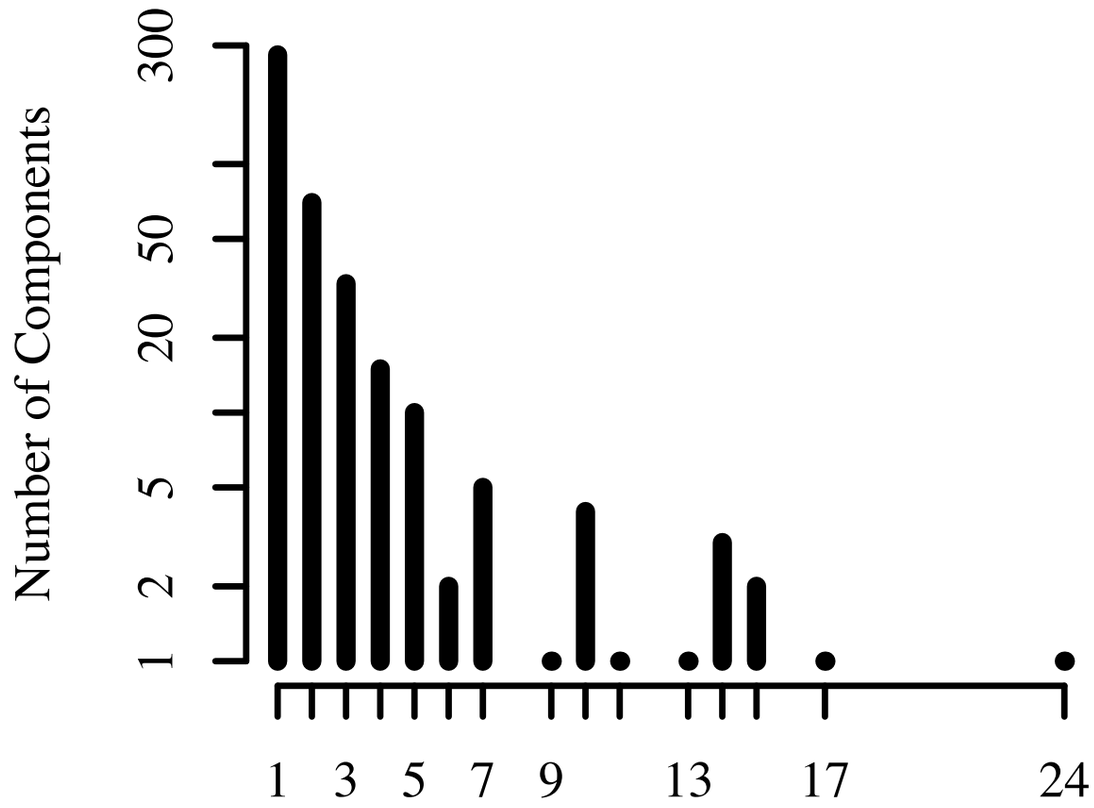

Mozilla Vulnerabilities
security
nss
lib
libpkix
pkix_pl_nss
modu
pki
sy
pkix
top
uti
r
incl
freebl
mpi
ecl
softoken
ssl
util
certd
smim
crmf
pki
pkcs
de
pk11wr
pkcs12
jar
cry
pki1
certhig
bas
asn
ckfw
builtins
ca
ns
cmd
zlib
lib
m
pk
si
fips
pk
ce
c
crlu
blt
S
t
manager
jss
org
s
layout
generic
style
xul
base
src
tr
tables
mathml
forms
base
src
svg
base
re
prin
in
ht
bu
base
mailnews
base
src
util
search
src
imap
src
addrbook
src
compose
src
import
outl
src
eud
oex
mime
src
local
src
news
src
exten
palm
b
s
mapi
old
ma
db
b
modules
oji
tests
sr
src
JNI
C
Arr
A
C
Ac
pu
plugin
tools
sam
test
s
s
def
base
src
S
libimg
png
libfont
jmcge
src
libpr0n
dec
s
zlib
src
rdf
src
softupd
src
libre
src
libp
src
libb
src
libjar
xml
s
li
pro
gfx
src
ps
xlib
mac
theb
xlib
qt
phot
gtk
windo
os2
be
xp
sh
x11sh
xpr
f
cairo
cairo
src
glitz
src
libpixma
src
thebe
src
publi
publ
js
src
xpconnect
src
test
l
liveco
fdlib
tamarin
core
pcre
code
MM
shell
pl
e
jsd
content
base
src
p
html
content
src
doc
src
xslt
src
xslt
xpath
xul
temp
src
doc
src
cont
svg
content
src
events
src
xbl
src
xml
d
xtf
can
xpcom
io
glue
reflect
xptcal
x
src
s
string
pu
sr
typelib
xpi
x
base
tests
ds
build
compo
obsolete
c
MoreFi
thr
pr
s
widget
src
mac
gtk2
windows
os2
beos
xpwi
qt
ph
gtk
xlib
co
g
g
embedding
browser
activex
src
co
co
plu
pl
gtk
src
phot
web
powerp
qt
compon
printin
win
fi
web
qa
teste
tests
mfc
w
directory
c-sdk
ldap
libraries
clie
i
libldap
exa
suncsdk
c-sdk
ldap
libraries
cli
i
xp
b
intl
uconv
ucvlat
src
uti
ucv
u
u
t
ucvcn
u
unichar
src
locale
src
ctl
src
chardet
src
l
s
netwerk
base
src
protocol
http
ftp
src
streamco
cache
test
dns
co
bui
s
java
webclient
src_moz
pluggab
wf
xpcom
te
ja
u
do
plu
jni
db
sqlite3
src
mork
src
tri
sr
md
editor
libeditor
html
base
text
txm
com
txtsv
calendar
libical
src
libical
libic
au
test
base
js2
src
re
browser
components
places
migrat
src
boo
s
extensions
canvas3d
src
xforms
webservice
soap
pro
sche
w
i
java
xpcom
xmlterm
base
line
python
xpco
walle
src
univ
src
spellch
src
sche
src
met
pre
ins
typ
sr
aut
w
s
p
sql
b
coo
s
xm
l
ef
Compiler
Code
md
x
Front
Primi
Runtim
Syste
gc
sr
i
C
N
C
Tools
Utilitie
Gener
zli
qa
c
Pack
co
D
Ex
D
xpinstall
wizard
windows
setup
uni
libxpne
GUSI
mac
os2
setup
unix
src
toolkit
components
place
src
his
s
do
pa
airbag
airbag
xre
m
xpfe
compone
sear
boo
hi
st
bootstra
app
appshel
nsprpub
pr
src
md
wi
uni
ma
o
b
misc
pthre
thr
cp
io
li
tests
include
md
p
li
t
li
parser
htmlparser
src
p
expa
lib
tools
trace-
li
codes
re
re
d
f
p
le
jp
accessible
src
atk
bas
ht
xu
ms
dom
src
base
other-license
7zst
src
7zi
libart_
atk-1.
jpeg
msgsdk
C
protocol
cck
expat
muc
driver
ib
gc
boehm
c
plugin
oji
MRJ
plu
MRJ
pl
rdf
base
chro
src
d
docshell
base
s
uriloader
extha
b
camino
src
ipc
ipcd
e
lib
mac
profile
sr
config
mston
src
view
src
mail
com
buil
win
dbm
s
i
sun
stu
web
w
sto
caps
src
gcon
sr
mini
chro


Mozilla Vulnerabilities
js
src
xpconnect
src
livecon
content
base
src
public
xbl
src
xul
document
src
p
content
src
templates
src
events
src
public
xslt
src
xslt
base
xml
document
src
svg
conte
content
src
canvas
src
html
content
src
documen
src
layout
xul
base
src
tree
src
grid
generic
base
forms
tables
style
build
mathm
printin
svg
html
dom
src
base
js
e
public
netwerk
protocol
http
src
about
view
base
src
streamc
convert
cache
dn
src
s
widget
src
mac
windows
pu
gtk
xlib
os2
gtk2
qt
phot
beos
xpwi
caps
src
inclu
xpinstall
src
uriloader
exthandler
un
os2
wi
be
mac
base
parser
expat
lib
htmlp
src
embedding
components
br
windoww
c
w
src
editor
libeditor
c
html
ba
te
security
nss
lib
util
softoken
ssl
cryptohi
pki
free
cert
pk1
smi
cmd
manager
boot
ssl
modules
plugin
base
libpr0n
decod
gif
x
libjar
oji
docshell
base
xpfe
appshell
co
src
se
hi
extensions
xforms
sq
b
toolkit
components
satch
hi
au
xpcom
string
public
src
io
glue
mailnews
base
src
se
addrb
src
mime
src
ne
sr
gfx
cairo
sr
cairo
intl
unich
uc
sr
ut
sr
view
src
p
acces
src
b
x
rdf
base
chro
storage
src
db
calen
brows
ipc
chrome
src
camin
webs

Distribution of MFSAs



Distribution of Bug Reports

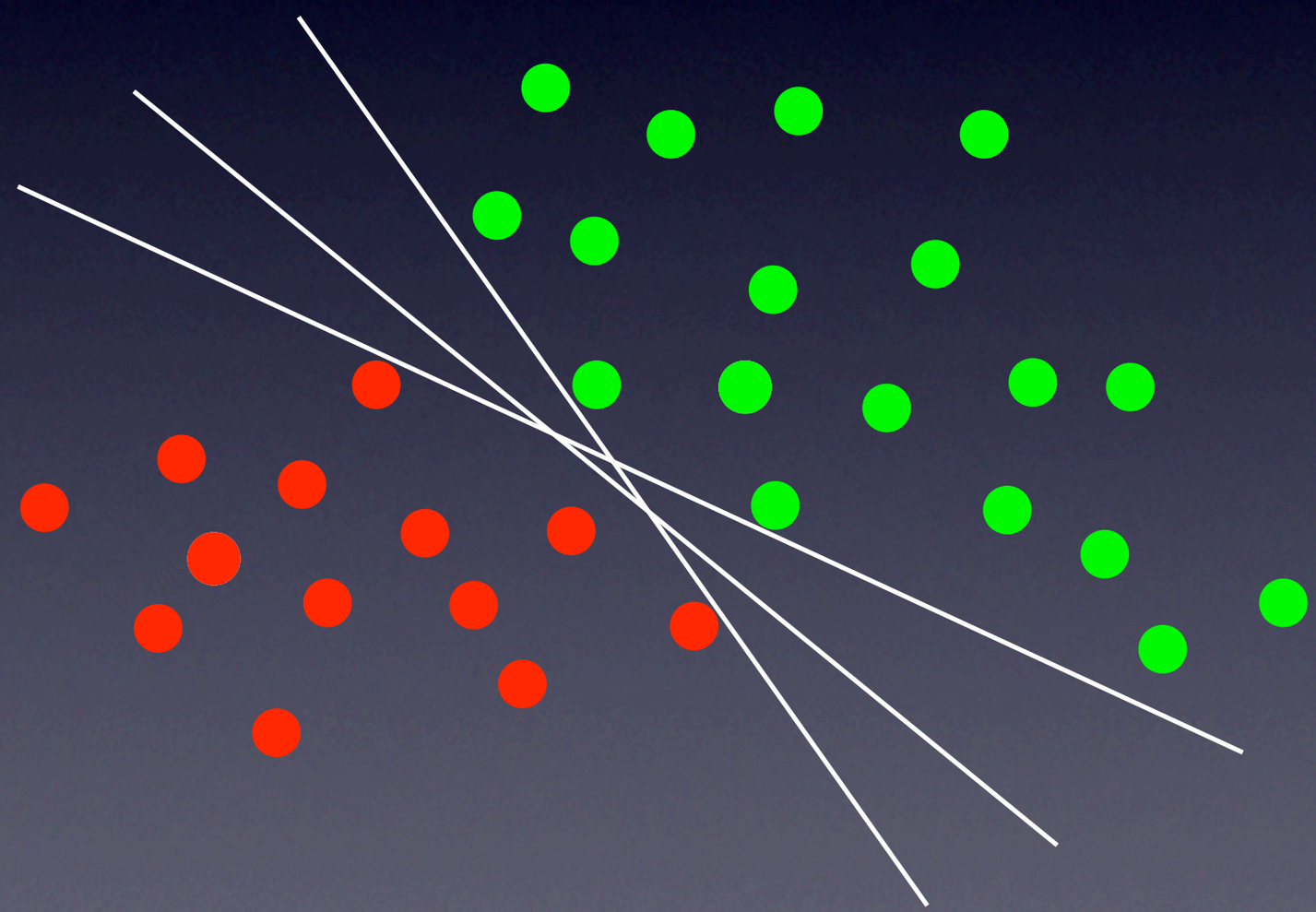


Imports

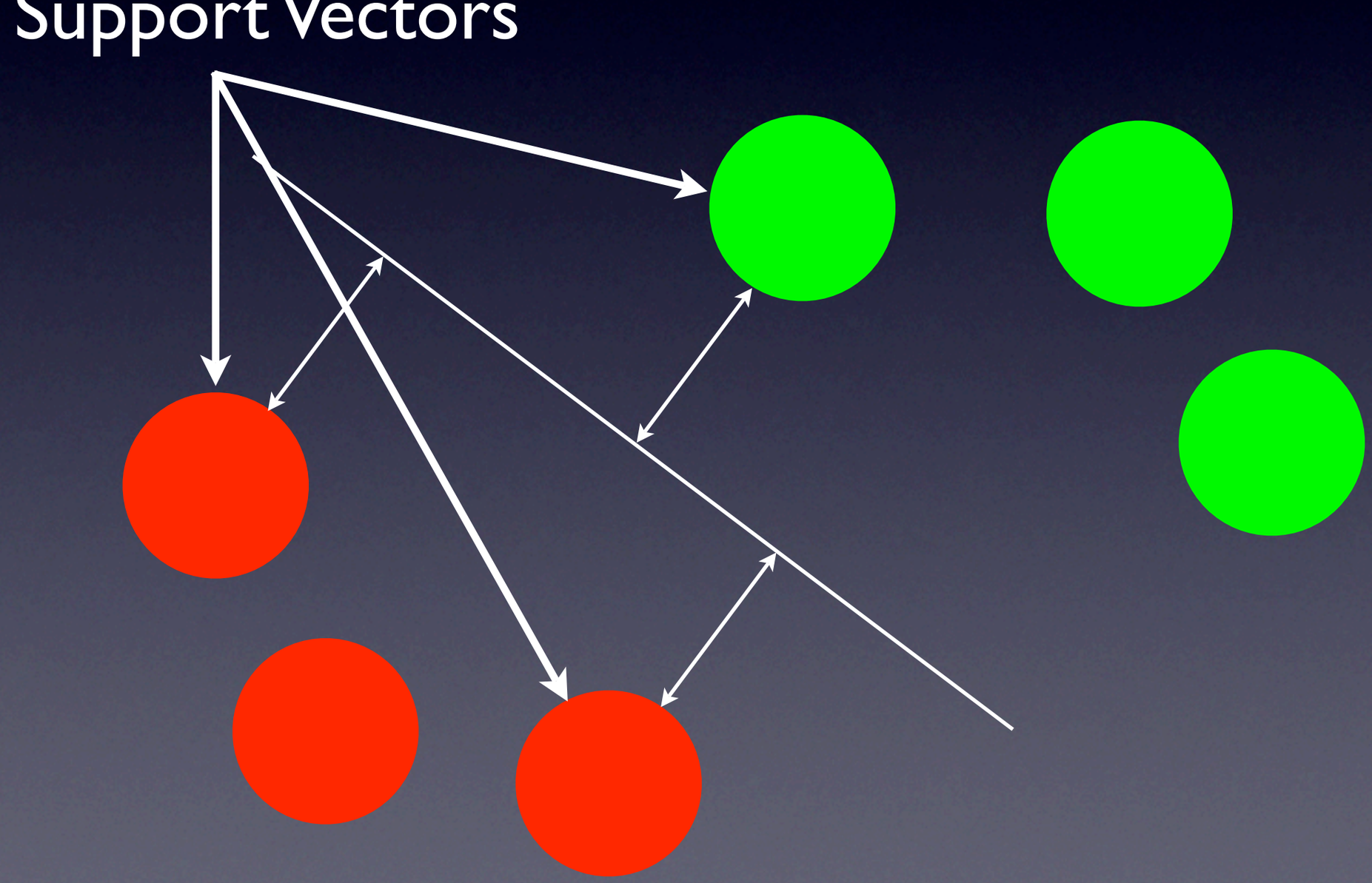
- 9,066 imports
- 79,541 import relations (*x* imports *y*)
- Takes about five minutes to compute

Results soon

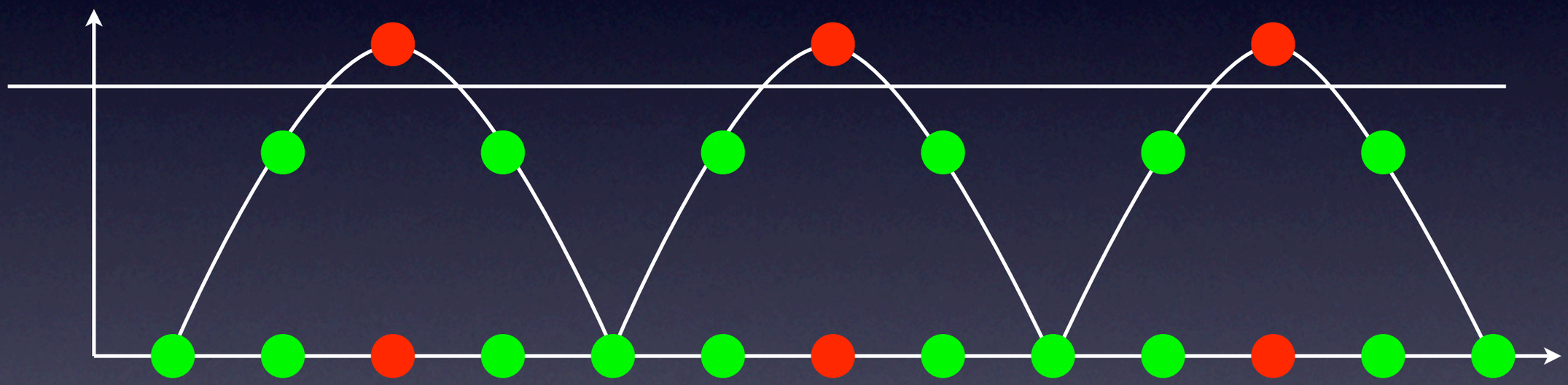
Support Vector Machines



Support Vector Machines



Support Vector Machines

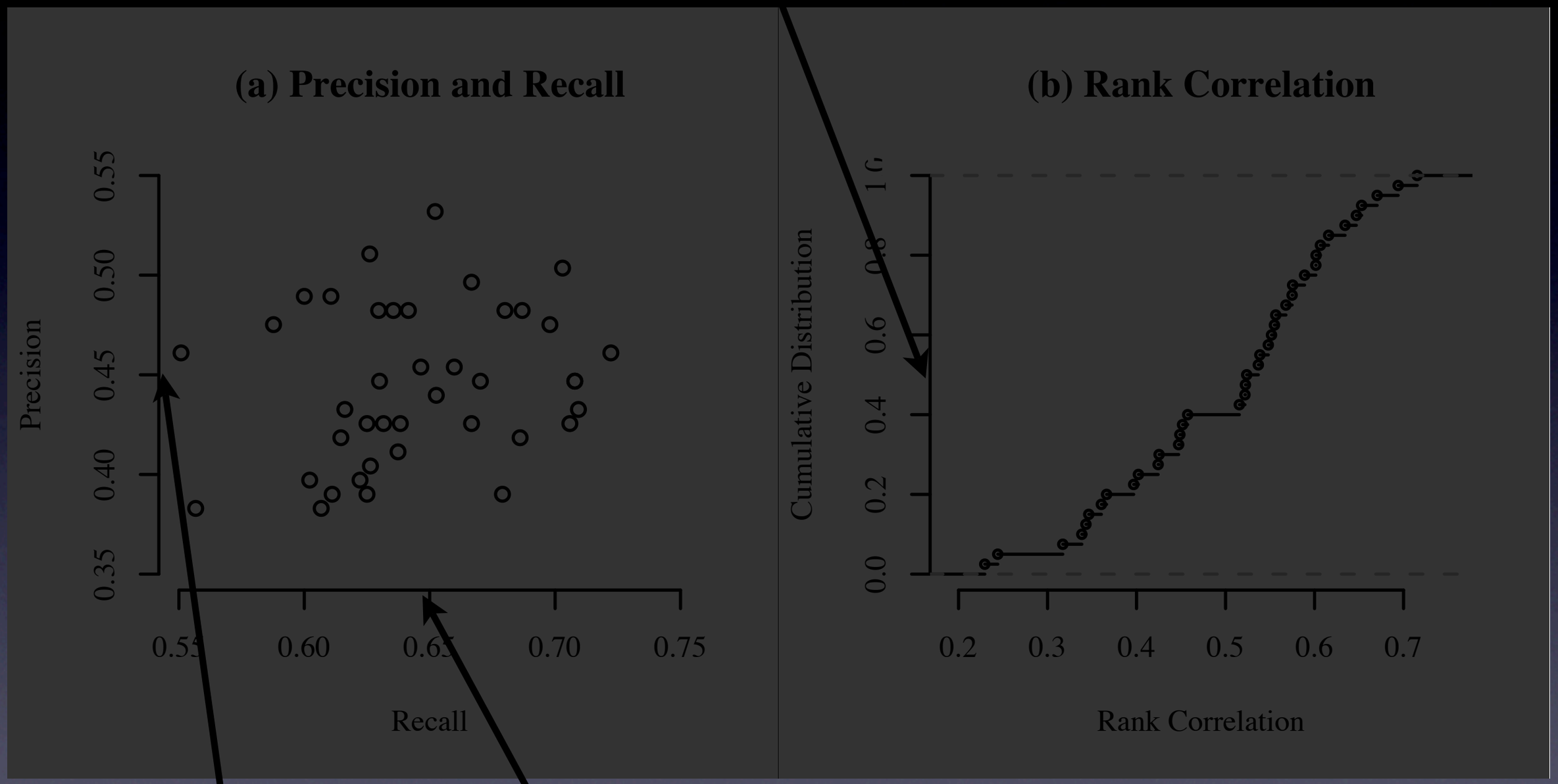


Results Now!

Experiments

- 40 random splits
  6,968 rows in training set, 3,484 rows in validation set
- Classification
  Train SVM, compute recall and precision
- Regression
  Train SVM, compute rank correlation on top 1%
- SVM: linear kernel with default parameters
  R implementation (up to 10GB of main memory)

moderately strong correlation (mostly significant at p < 0.01)



2/3 of all vulnerable components detected

45% (about 1/2) of predictions correct

Similar Results for Bugs

Packages + Import relationships

(Schröter et al, ISESE 2006)

Precision: 66.7% Recall: 69.4%

Binaries + Dependencies

(Zimmermann/Nagappan @ Microsoft Research, 2006)

Precision: 64.4% Recall: 75.3%

Predicted Rank	Component	Actual Rank
1	nsDOMClassInfo	3
2	SGridRowLayout	95
3	xpcprivate	6
4	jsxml	2
5	nsGenericHTMLElement	8
6	jsgc	3
7	nsISEnvironment	12
8	jsfun	1
9	nsHTMLLabelElement	18
10	nsHttpTransaction	35