

Chasing a 25 year old Thunderbird security bug

Garmin Sam, Douglas Bagnall

File Edit View Go Message Enigmail Tools Help

Get Messages Write Chat Address Book Tag

From Me <garming@catalyst.net.nz>★

Reply

Reply All

Forward

More

Subject Patch to pass a Windows RODC test

20/09/16 17:33

To Catalyst Samba Developers <samba-dev@catalyst.net.nz>★

Things to do:

- Automate credentials pre-loading in RODC environments (add Administrator to RODC replication group + RODC preload run)
- Give a proper server for the referrals (PDC or replication partner instead of hardcoding)
- Add the same check in the deleted case

—0001-Let-me-cheat-here.patch—

From eeba21f2bf1fb4a28d498ba032edcb8625eb68c7 Mon Sep 17 00:00:00 2001

From: Ubuntu <ubuntu@gar-mas-0-2.samdom.example.com>

Date: Tue, 20 Sep 2016 04:25:34 +0000

Subject: [PATCH] Let me cheat here...

Signed-off-by: Ubuntu <ubuntu@gar-mas-0-2.samdom.example.com>

```
source4/dsdb/samdb/ldb_modules/repl_meta_data.c | 25 +++++
source4/dsdb/samdb/ldb_modules/samldb.c         | 10 +++++
2 files changed, 35 insertions(+)
```

diff --git a/source4/dsdb/samdb/ldb_modules/repl_meta_data.c b/source4/dsdb/samdb/ldb_modules/repl_meta_data.c

index 7a5906e..d870479 100644

--- a/source4/dsdb/samdb/ldb_modules/repl_meta_data.c

+++ b/source4/dsdb/samdb/ldb_modules/repl_meta_data.c

@@ -976,6 +976,30 @@ static int replmd_add(struct ldb_module *module, struct ldb_request *req)

guid = GUID_random();

}

```
+ if (!ldb_request_get_control(req, DSDB_CONTROL_REPLICATED_UPDATE_OID)
+     && !ldb_request_get_control(req, DSDB_CONTROL_DBCHECK_MODIFY_RO_REPLICA)) {
```

```
+     bool rodc = false;
+     struct loadparm_context *lp_ctx;
+     char *referral;
```

```
+     ret = samdb_rodc(ldb, &rodc);
+     if (ret != LDB_SUCCESS) {
+         DEBUG(4, (__location__ ": unable to tell if we are an RODC\n"));
+     } else if (rodc) {
```

```
+         ldb_set_errstring(ldb, "RODC modify is forbidden!");
+         lp_ctx = talloc_get_type(ldb_get_opaque(ldb, "loadparm"),
+                                 struct loadparm_context);
```

```
+         referral = talloc_asprintf(req,
+                                     "ldap://gar-mas-0-0.%s/%s",
+                                     lp_ctx->dnsdomain, lp_ctx->name);
```

To: Catalyst Samba Developers <samba-dev@catalyst.net.nz>
From: Garming Sam <garming@catalyst.net.nz>
Subject: Patch to pass a Windows RODC test
Message-ID: <3ae65b63-914e-27ac-f39a-3e071156f597@catalyst.net.nz>
Date: Tue, 20 Sep 2016 17:33:01 +1200
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Thunderbird/45.2.0
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="-----C2AFA65155D3EB764BFA8504"

This is a multi-part message in MIME format.

-----C2AFA65155D3EB764BFA8504

Content-Type: text/plain; charset=utf-8

Content-Transfer-Encoding: 7bit

Things to do:

- Automate credentials pre-loading in RODC environments (add Administrator to RODC replication group + RODC preload run)
- Give a proper server for the referrals (PDC or replication partner instead of hardcoding)
- Add the same check in the deleted case

-----C2AFA65155D3EB764BFA8504

Content-Type: text/x-diff;

name="0001-Let-me-cheat-here.patch"

Content-Transfer-Encoding: 7bit

Content-Disposition: attachment;

filename="0001-Let-me-cheat-here.patch"

From eebe21f2bf1fb4a28d498ba032edcb8625eb68c7 Mon Sep 17 00:00:00 2001

From: Ubuntu <ubuntu@gar-mas-0-2.samdom.example.com>

Date: Tue, 20 Sep 2016 04:25:34 +0000

Subject: [PATCH] Let me cheat here...

Signed-off-by: Ubuntu <ubuntu@gar-mas-0-2.samdom.example.com>

```
source4/dsdb/samdb/ldb_modules/repl_meta_data.c | 25 ++++++
source4/dsdb/samdb/ldb_modules/samldb.c         | 10 +++++
2 files changed, 35 insertions(+)
```

Options?

Strategy 0: Ignore it

Strategy 1: GDB, standard debugger

Strategy 2: Valgrind

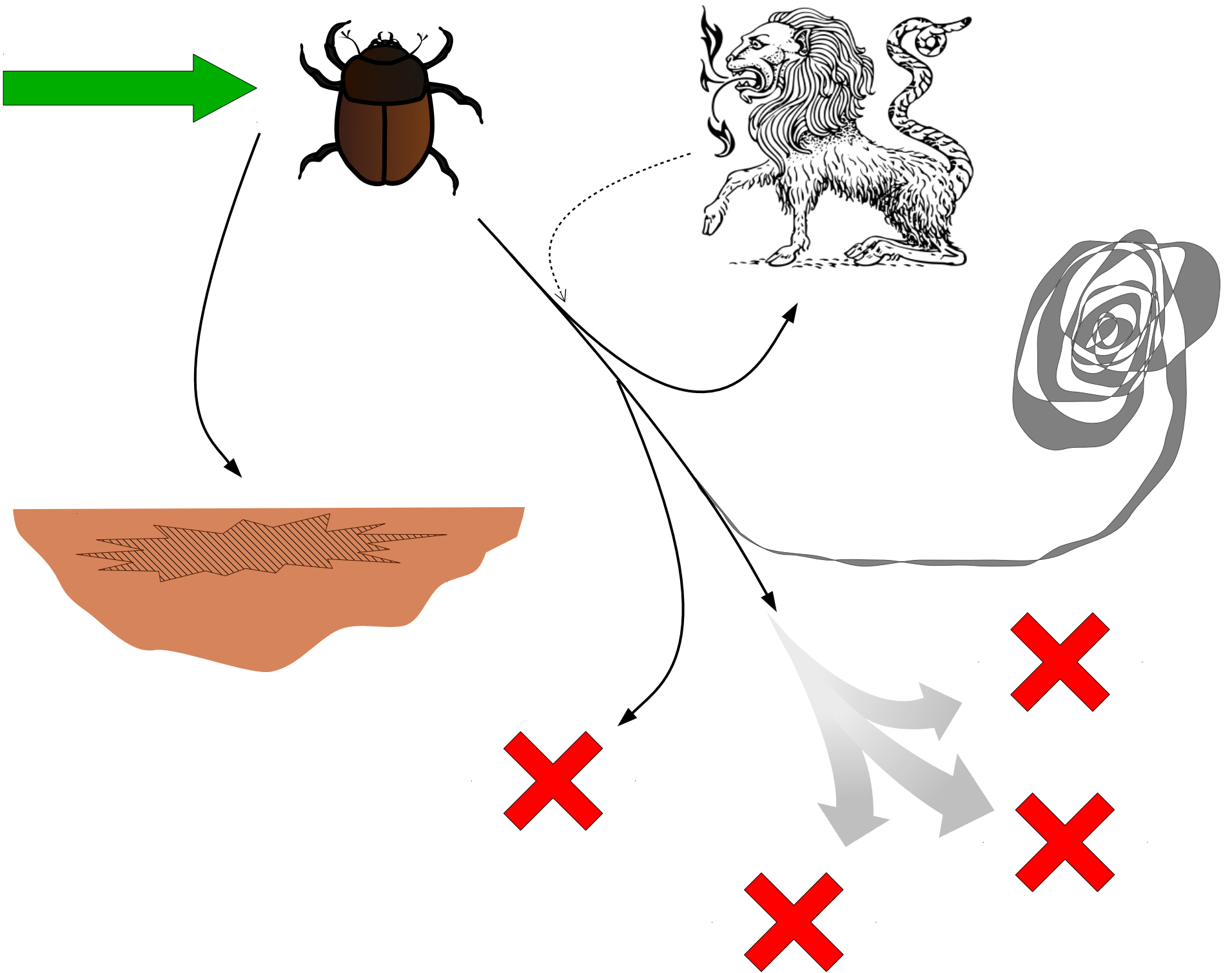
Strategy 3: Address Sanitizer

Strategy 4: Bisection of input

Strategy 5: ???

GDB (Standard debugger)

- + Works well for master diviners, super sleuths, and those-who-know-the-entire-project
- Needs symbols to be effective, building from scratch and lots of code navigation
- + Allows useful data extraction of the actual crash
- Gives no clues as to what the cause is



Hints so far

Crash signatures:

arena_malloc | nsStringBuffer::Alloc | MimeInlineText_parse_eof

0x0 | CanonicalizeXPComParticipant | nsCycleCollector::ForgetSkippable

arena_dalloc | nsLDAPURL::Init | js::RunScript

arena_dalloc | GetMsgDBHdrFromURI | nsMailboxUrl::GetFolder

Memory corruption likely in email parsing (specifically in the attachment)

Scattered crashes in GC + memory alloc + JIT + XPCOM + parsing

Previous bugs had been found in parsing mime contents

```
==12752== by 0xF234569: mozJSCComponentLoader::ObjectForLocation(ComponentLoaderInfo&, nsIFile*,
JS::MutableHandle<JSObject*>, JS::MutableHandle<JSScript*>, char**, bool, JS::MutableHandle<JS::Value>)
(mozJSCComponentLoader.cpp:684)
==12752== by 0xF235710: mozJSCComponentLoader::LoadModule(mozilla::FileLocation&)
(mozJSCComponentLoader.cpp:390)
==12752== by 0xE9D17A8: nsComponentManagerImpl::KnownModule::Load()
(nsComponentManager.cpp:832)
==12752== by 0xE9D182A: nsFactoryEntry::GetFactory() (nsComponentManager.cpp:1865)
==12752== Address 0x1f277858 is 8 bytes after a block of size 32 free'd
==12752== at 0x923318F: g_type_free_instance (in /usr/lib/x86_64-linux-gnu/libgobject-2.0.so.0.4002.0)
==12752== by 0x689A561: ??? (in /usr/lib/x86_64-linux-gnu/libgtk-3.so.0.1000.8)
==12752== by 0x9218ACF: g_object_run_dispose (in /usr/lib/x86_64-linux-gnu/libgobject-2.0.so.0.4002.0)
==12752== by 0x686A0FF: ??? (in /usr/lib/x86_64-linux-gnu/libgtk-3.so.0.1000.8)
==12752== by 0x6861F07: ??? (in /usr/lib/x86_64-linux-gnu/libgtk-3.so.0.1000.8)
==12752== by 0x9212331: g_closure_invoke (in /usr/lib/x86_64-linux-gnu/libgobject-2.0.so.0.4002.0)
==12752== by 0x92240D3: ??? (in /usr/lib/x86_64-linux-gnu/libgobject-2.0.so.0.4002.0)
==12752== by 0x922BA28: g_signal_emit_valist (in /usr/lib/x86_64-linux-gnu/libgobject-2.0.so.0.4002.0)
==12752== by 0x922BCE1: g_signal_emit (in /usr/lib/x86_64-linux-gnu/libgobject-2.0.so.0.4002.0)
==12752== by 0x6A30A57: ??? (in /usr/lib/x86_64-linux-gnu/libgtk-3.so.0.1000.8)
==12752== by 0x9218ACF: g_object_run_dispose (in /usr/lib/x86_64-linux-gnu/libgobject-2.0.so.0.4002.0)
==12752== by 0x68BB73F: ??? (in /usr/lib/x86_64-linux-gnu/libgtk-3.so.0.1000.8)
==12752==
==12752== Invalid read of size 8
==12752== at 0xF284891: XPCWrappedNative::Init(XPCNativeScriptableCreateInfo const*)
(XPCWrappedNative.cpp:761)
==12752== by 0xF292BF5: XPCWrappedNative::GetNewOrUsed(xpcObjectHelper&,
XPCWrappedNativeScope*, XPCNativeInterface*, XPCWrappedNative**) (XPCWrappedNative.cpp:455)
==12752== by 0xF268F0E: XPCConvert::NativeInterface2JSObject(JS::MutableHandle<JS::Value>,
nsIXPCConnectJSObjectHolder**, xpcObjectHelper&, nsID const*, bool, nsresult*) (XPCConvert.cpp:829)
==12752== by 0xF283F07:
XPCWrappedNativeScope::GetComponentsJSObject(JS::MutableHandle<JSObject*>)
(XPCWrappedNativeScope.cpp:199)
==12752== by 0xF285CB0: XPCWrappedNativeScope::AttachComponentsObject(JSContext*)
(XPCWrappedNativeScope.cpp:226)
==12752== by 0xF285EAC: xpc::InitGlobalObject(JSContext*, JS::Handle<JSObject*>, unsigned int)
(nsXPConnect.cpp:466)
==12752== by 0xF2922BE: nsXPConnect::InitClassesWithNewWrappedGlobal(JSContext*, nsISupports*,
nsIPrincipal*, unsigned int, JS::CompartmentOptions&, nsIXPCConnectJSObjectHolder**)
```



```
==12752== by 0x92240D3: ??? (in /usr/lib/x86_64-linux-gnu/libgobject-2.0.so.0.4002.0)
==12752== by 0x922BA28: g_signal_emit_valist (in /usr/lib/x86_64-linux-gnu/libgobject-2.0.so.0.4002.0)
==12752== by 0x922BCE1: g_signal_emit (in /usr/lib/x86_64-linux-gnu/libgobject-2.0.so.0.4002.0)
==12752== by 0x6A30A57: ??? (in /usr/lib/x86_64-linux-gnu/libgtk-3.so.0.1000.8)
==12752== by 0x9218ACF: g_object_run_dispose (in /usr/lib/x86_64-linux-gnu/libgobject-2.0.so.0.4002.0)
==12752== by 0x68BB73F: ??? (in /usr/lib/x86_64-linux-gnu/libgtk-3.so.0.1000.8)
==12752==
==12752== Invalid read of size 8
==12752== at 0xF2958DB: IsTaggedScope (xpcprivate.h:1756)
==12752== by 0xF2958DB: HasProto (xpcprivate.h:1772)
==12752== by 0xF2958DB: XPCWrappedNative::GetProto() const (xpcprivate.h:1776)
==12752== by 0xF284A40: XPCWrappedNative::Init(XPCNativeScriptableCreateInfo const*)
(XPCWrappedNative.cpp:781)
==12752== by 0xF292BF5: XPCWrappedNative::GetNewOrUsed(xpcObjectHelper&,
XPCWrappedNativeScope*, XPCNativeInterface*, XPCWrappedNative**) (XPCWrappedNative.cpp:455)
==12752== by 0xF268F0E: XPCConvert::NativeInterface2JSObject(JS::MutableHandle<JS::Value>,
nsIXPCConnectJSObjectHolder**, xpcObjectHelper&, nsID const*, bool, nsresult*) (XPCConvert.cpp:829)
==12752== by 0xF283F07:
XPCWrappedNativeScope::GetComponentsJSObject(JS::MutableHandle<JSObject*>)
(XPCWrappedNativeScope.cpp:199)
==12752== by 0xF285CB0: XPCWrappedNativeScope::AttachComponentsObject(JSContext*)
(XPCWrappedNativeScope.cpp:226)
==12752== by 0xF285EAC: xpc::InitGlobalObject(JSContext*, JS::Handle<JSObject*>, unsigned int)
(nsXPConnect.cpp:466)
==12752== by 0xF2922BE: nsXPConnect::InitClassesWithNewWrappedGlobal(JSContext*, nsISupports*,
nsIPrincipal*, unsigned int, JS::CompartmentOptions&, nsIXPCConnectJSObjectHolder**)
(nsXPConnect.cpp:513)
==12752== by 0xF233530: mozJSComponentLoader::PrepareObjectForLocation(JSContext*, nsIFile*,
nsIURI*, bool, bool*) (mozJSComponentLoader.cpp:581)
==12752== by 0xF234569: mozJSComponentLoader::ObjectForLocation(ComponentLoaderInfo&, nsIFile*,
JS::MutableHandle<JSObject*>, JS::MutableHandle<JSScript*>, char**, bool, JS::MutableHandle<JS::Value>)
(mozJSComponentLoader.cpp:684)
==12752== by 0xF235710: mozJSComponentLoader::LoadModule(mozilla::FileLocation&)
(mozJSComponentLoader.cpp:390)
==12752== by 0xE9D17A8: nsComponentManagerImpl::KnownModule::Load()
(nsComponentManager.cpp:832)
==12752== Address 0x1f277840 is 16 bytes inside a block of size 32 free'd
==12752== at 0x923318F: g_type_free_instance (in /usr/lib/x86_64-linux-gnu/libgobject-2.0.so.0.4002.0)
```

```
==12752== by 0xF292BF5: XPCWrappedNative::GetNewOrUsed(xpcObjectHelper&,
XPCWrappedNativeScope*, XPCNativeInterface*, XPCWrappedNative**) (XPCWrappedNative.cpp:455)
==12752== by 0xF268F0E: XPCConvert::NativeInterface2JSObject(JS::MutableHandle<JS::Value>,
nsIXPCConnectJSObjectHolder**, xpcObjectHelper&, nsID const*, bool, nsresult*) (XPCConvert.cpp:829)
==12752== by 0xF283F07:
XPCWrappedNativeScope::GetComponentsJSObject(JS::MutableHandle<JSObject*>)
(XPCWrappedNativeScope.cpp:199)
==12752== by 0xF285CB0: XPCWrappedNativeScope::AttachComponentsObject(JSContext*)
(XPCWrappedNativeScope.cpp:226)
==12752== by 0xF285EAC: xpc::InitGlobalObject(JSContext*, JS::Handle<JSObject*>, unsigned int)
(nsXPConnect.cpp:466)
==12752== by 0xF2922BE: nsXPConnect::InitClassesWithNewWrappedGlobal(JSContext*, nsISupports*,
nsIPrincipal*, unsigned int, JS::CompartmentOptions&, nsIXPCConnectJSObjectHolder**)
(nsXPConnect.cpp:513)
==12752== by 0xF233530: mozJSComponentLoader::PrepareObjectForLocation(JSContext*, nsIFile*,
nsIURI*, bool, bool*) (mozJSComponentLoader.cpp:581)
==12752== by 0xF234569: mozJSComponentLoader::ObjectForLocation(ComponentLoaderInfo&, nsIFile*,
JS::MutableHandle<JSObject*>, JS::MutableHandle<JSScript*>, char**, bool, JS::MutableHandle<JS::Value>)
(mozJSComponentLoader.cpp:684)
==12752== by 0xF235710: mozJSComponentLoader::LoadModule(mozilla::FileLocation&)
(mozJSComponentLoader.cpp:390)
==12752== by 0xE9D17A8: nsComponentManagerImpl::KnownModule::Load()
(nsComponentManager.cpp:832)
==12752== Address 0x1f277850 is 0 bytes after a block of size 32 free'd
==12752== at 0x923318F: g_type_free_instance (in /usr/lib/x86_64-linux-gnu/libgobject-2.0.so.0.4002.0)
==12752== by 0x689A561: ??? (in /usr/lib/x86_64-linux-gnu/libgtk-3.so.0.1000.8)
==12752== by 0x9218ACF: g_object_run_dispose (in /usr/lib/x86_64-linux-gnu/libgobject-2.0.so.0.4002.0)
==12752== by 0x686A0FF: ??? (in /usr/lib/x86_64-linux-gnu/libgtk-3.so.0.1000.8)
==12752== by 0x6861F07: ??? (in /usr/lib/x86_64-linux-gnu/libgtk-3.so.0.1000.8)
==12752== by 0x9212331: g_closure_invoke (in /usr/lib/x86_64-linux-gnu/libgobject-2.0.so.0.4002.0)
==12752== by 0x92240D3: ??? (in /usr/lib/x86_64-linux-gnu/libgobject-2.0.so.0.4002.0)
==12752== by 0x922BA28: g_signal_emit_valist (in /usr/lib/x86_64-linux-gnu/libgobject-2.0.so.0.4002.0)
==12752== by 0x922BCE1: g_signal_emit (in /usr/lib/x86_64-linux-gnu/libgobject-2.0.so.0.4002.0)
==12752== by 0x6A30A57: ??? (in /usr/lib/x86_64-linux-gnu/libgtk-3.so.0.1000.8)
==12752== by 0x9218ACF: g_object_run_dispose (in /usr/lib/x86_64-linux-gnu/libgobject-2.0.so.0.4002.0)
==12752== by 0x68BB73F: ??? (in /usr/lib/x86_64-linux-gnu/libgtk-3.so.0.1000.8)
==12752==
==12752== Invalid write of size 8
```

Valgrind (Runtime validator)

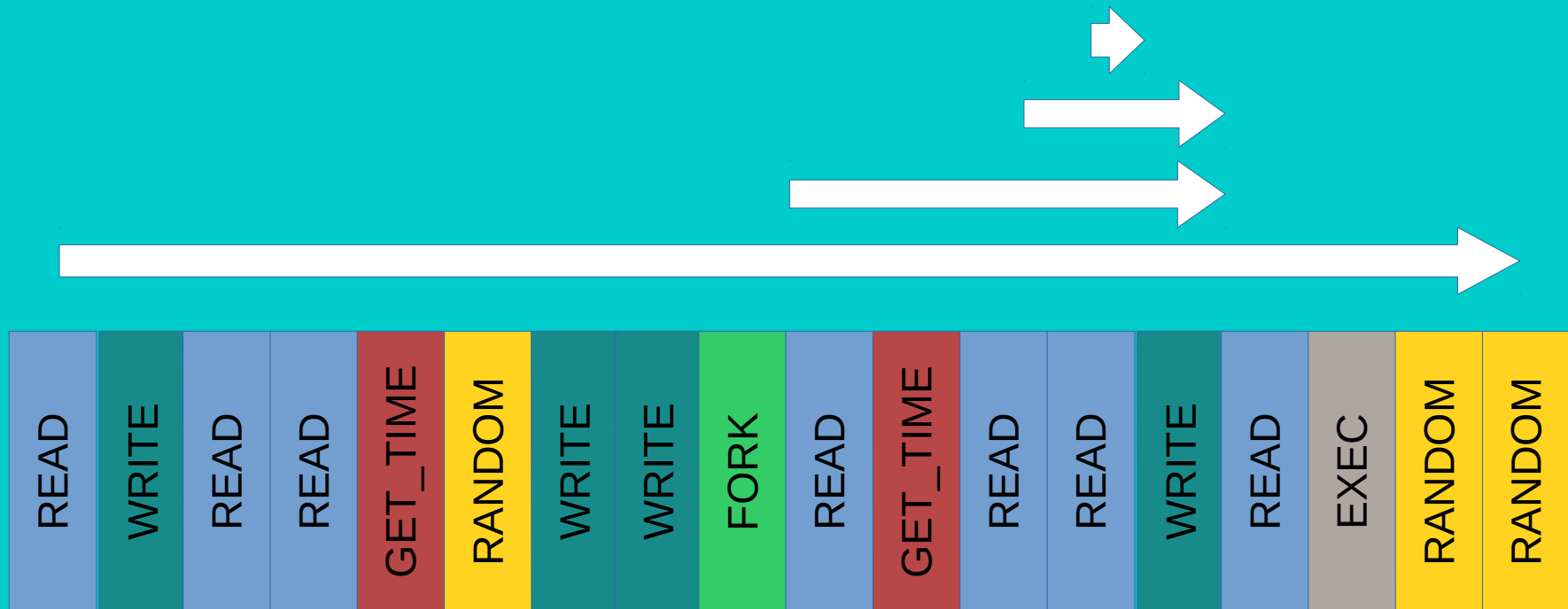
- + Will probably catch the bug
- Will also catch every other 'bug'
- + No need for recompilation
- Needs to be integrated into your project
- Supression files help, but not entirely
- Severe memory corruptions can crash valgrind
- Not considering giving up my will to live

Address Sanitizer (Runtime validator)

- Unlike Valgrind, needs to be compiled in
- Needs project and build system knowledge
- + Will catch lots of bugs
- Won't necessarily help you catch your bug
- No setup available for Thunderbird

Record-and-replay debugger (RR)

- Written by Robert O'Callahan, designed for Firefox
- Allows nearly real-time (1.0–1.5x) record and replay
- Uses CPU performance counters



Usage

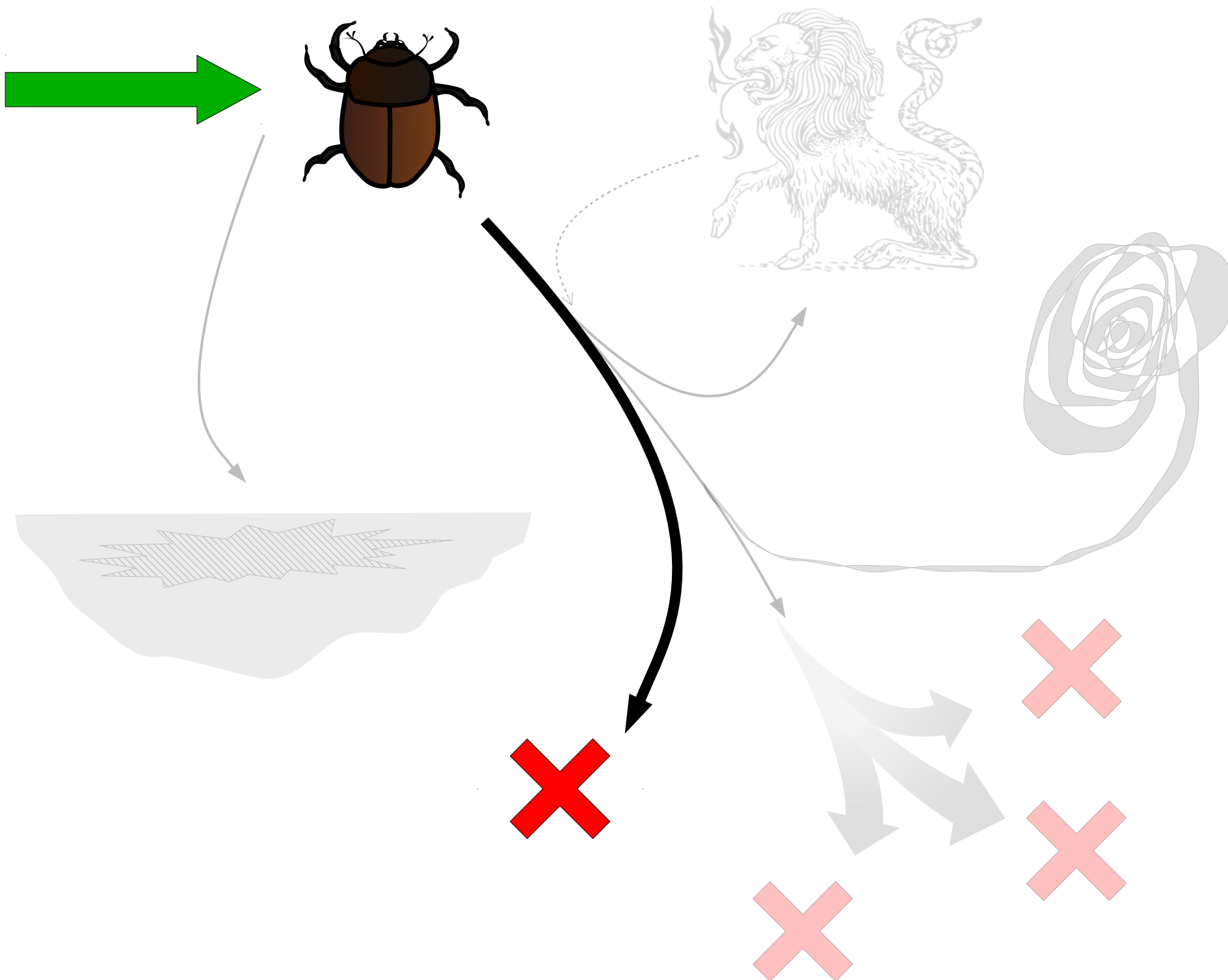
```
$> rr record thunderbird 'Patch to pass a Windows RODC test.eml'
```

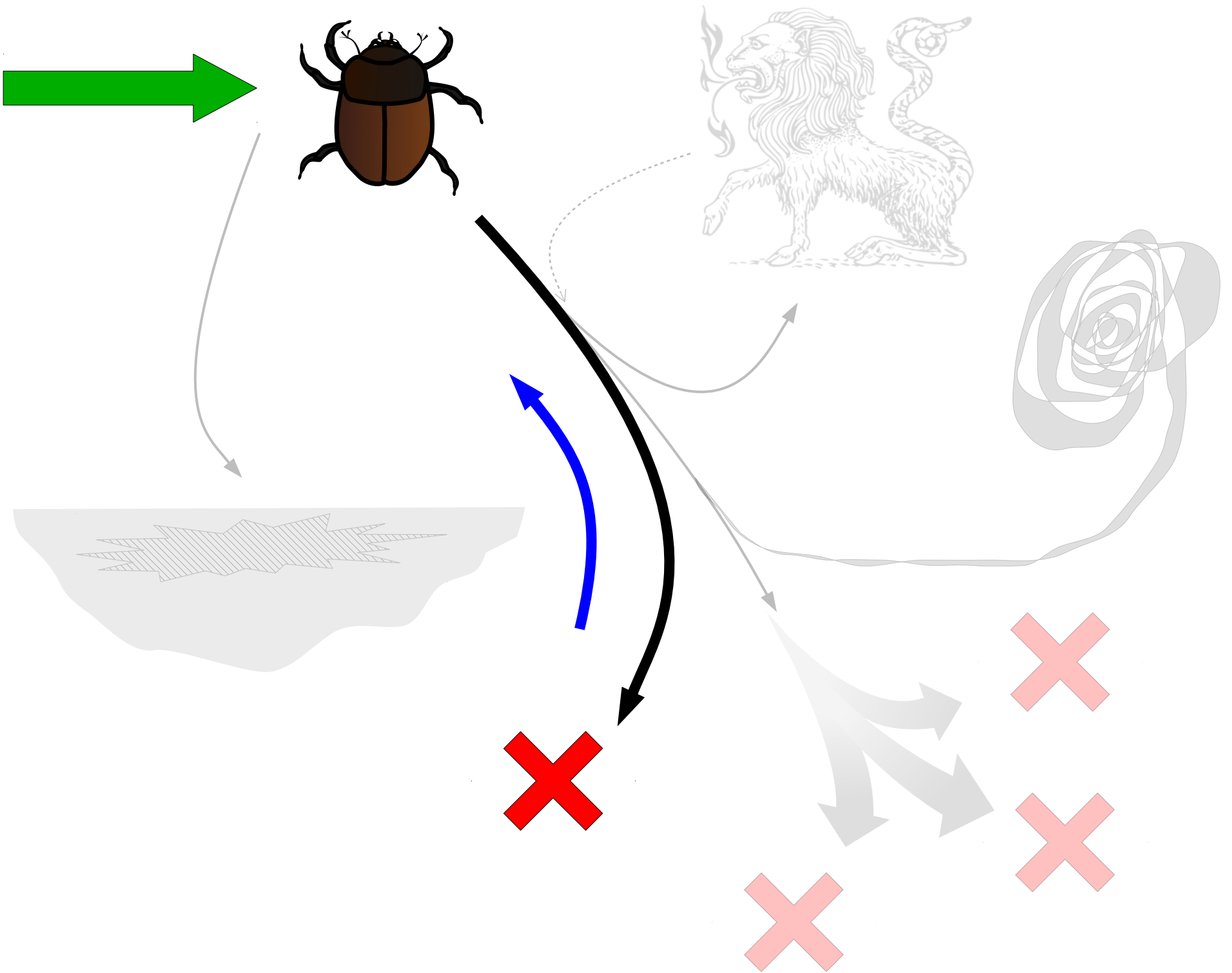
```
$> rr replay
```

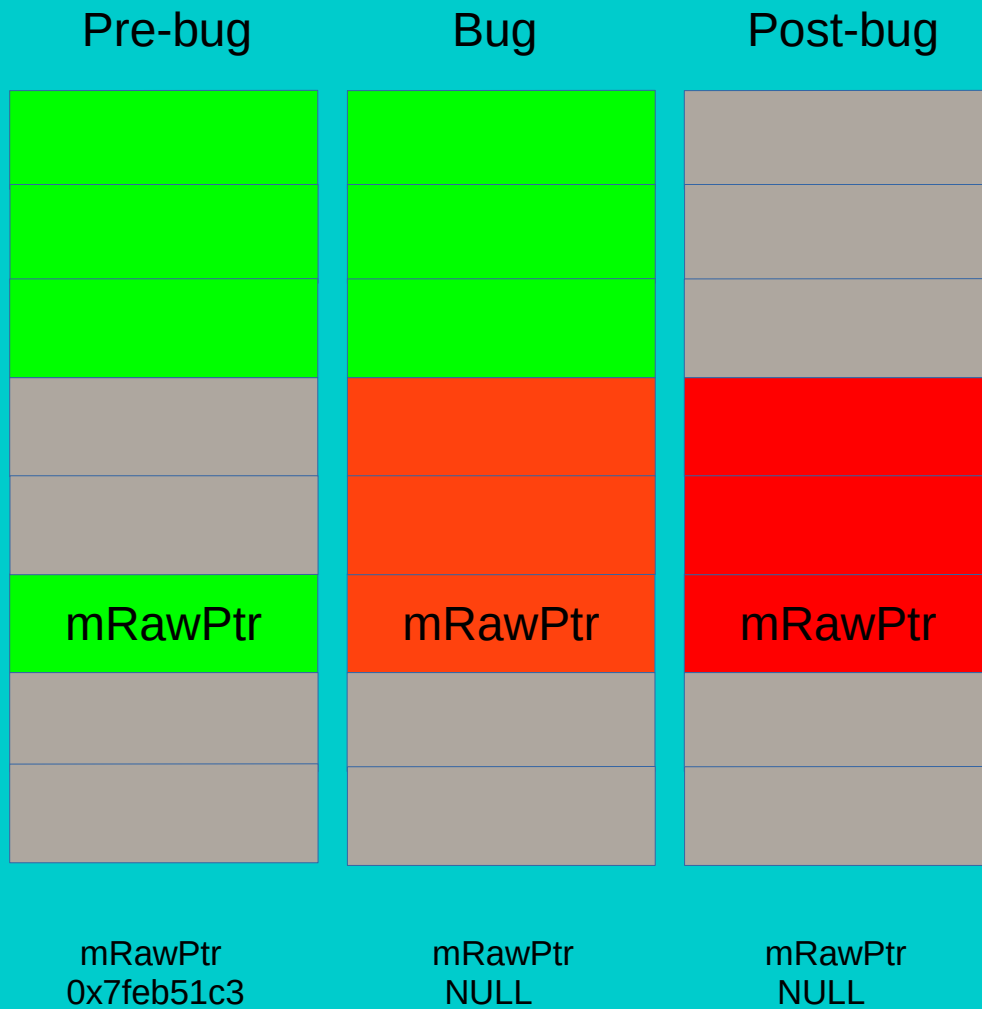
-M	displays event numbers
--goto <event number>	replay normally until an event
-p <PID>	attach on new process

New commands: reverse-next, reverse-step, reverse-continue, reverse-finish

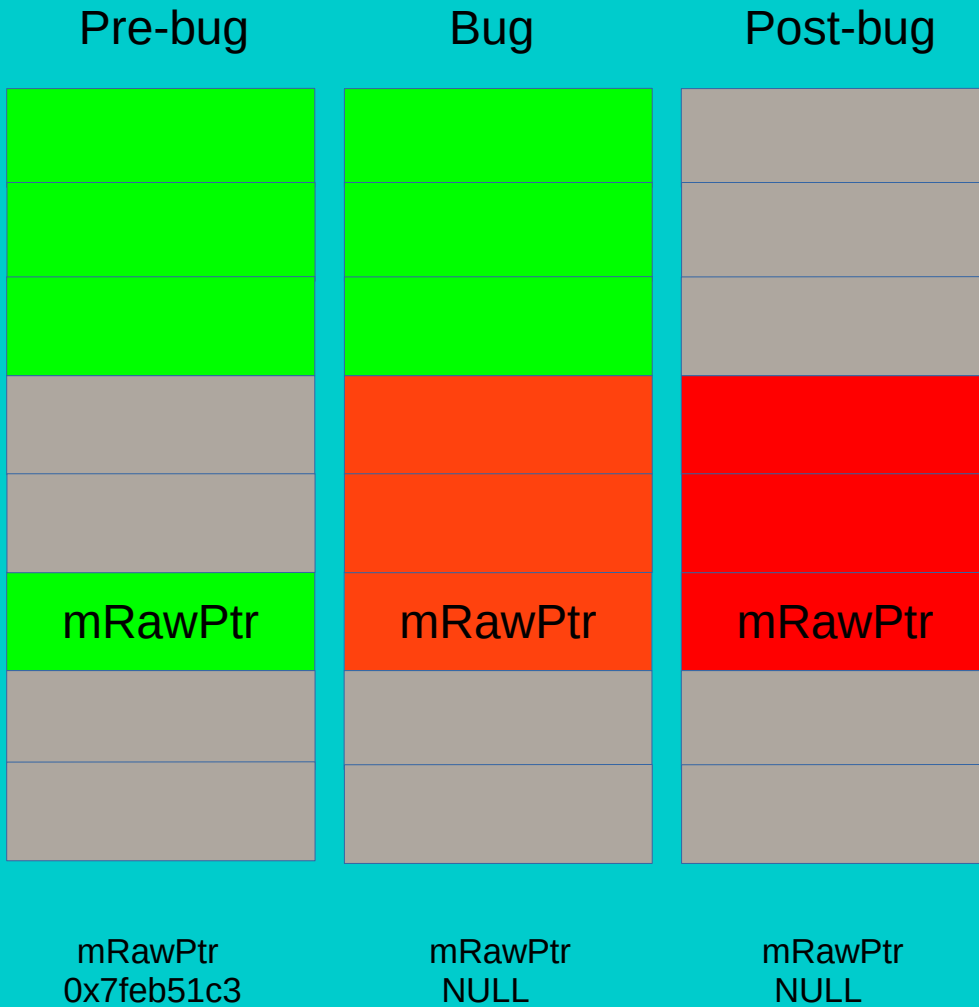
- + Completely deterministic (pids, addresses, registers)
- + No domain knowledge required
- + Replay repeatedly, can isolate cause from symptoms
- +/- Only native support for C, C++ and Rust







1. Thunderbird crash (SIGSEGV)
2. Set hardware watchpoint (mRawPtr)
3. Reverse-continue
4. Encounter exact location of bug



1. Thunderbird crash (SIGSEGV)
2. Set hardware watchpoint (mRawPtr)
3. Reverse-continue
4. Encounter exact location of bug

nsldapi_hex_unescape

File Edit View Go Message Enigmail Tools Help

Get Messages Write Chat Address Book Tag

From Me <garming@catalyst.net.nz>★

Reply

Reply All

Forward

More

Subject Patch to pass a Windows RODC test

20/09/16 17:33

To Catalyst Samba Developers <samba-dev@catalyst.net.nz>★

Things to do:

- Automate credentials pre-loading in RODC environments (add Administrator to RODC replication group + RODC preload run)
- Give a proper server for the referrals (PDC or replication partner instead of hardcoding)
- Add the same check in the deleted case

—0001-Let-me-cheat-here.patch—

From eeba21f2bf1fb4a28d498ba032edcb8625eb68c7 Mon Sep 17 00:00:00 2001

From: Ubuntu <ubuntu@gar-mas-0-2.samdom.example.com>

Date: Tue, 20 Sep 2016 04:25:34 +0000

Subject: [PATCH] Let me cheat here...

Signed-off-by: Ubuntu <ubuntu@gar-mas-0-2.samdom.example.com>

```
source4/dsdb/samdb/ldb_modules/repl_meta_data.c | 25 ++++++
source4/dsdb/samdb/ldb_modules/samldb.c         | 10 ++++++
2 files changed, 35 insertions(+)
```

diff --git a/source4/dsdb/samdb/ldb_modules/repl_meta_data.c b/source4/dsdb/samdb/ldb_modules/repl_meta_data.c

index 7a5906e..d870479 100644

--- a/source4/dsdb/samdb/ldb_modules/repl_meta_data.c

+++ b/source4/dsdb/samdb/ldb_modules/repl_meta_data.c

@@ -976,6 +976,30 @@ static int replmd_add(struct ldb_module *module, struct ldb_request *req)

guid = GUID_random();

}

```
+ if (!ldb_request_get_control(req, DSDB_CONTROL_REPLICATED_UPDATE_OID)
+     && !ldb_request_get_control(req, DSDB_CONTROL_DBCHECK_MODIFY_RO_REPLICA)) {
```

```
+     bool rodc = false;
+     struct loadparm_context *lp_ctx;
+     char *referral;
```

```
+     ret = samdb_rodc(ldb, &rodc);
+     if (ret != LDB_SUCCESS) {
+         DEBUG(4, (__location__ ": unable to tell if we are an RODC\n"));
+     } else if (rodc) {
```

```
+         ldb_set_errstring(ldb, "RODC modify is forbidden!");
+         lp_ctx = talloc_get_type(ldb_get_opaque(ldb, "loadparm"),
+                                 struct loadparm_context);
```

```
+         referral = talloc_asprintf(req,
+                                     "ldap://gar-mas-0-0.%s/%s",
+                                     lp_ctx->dnsdomain, lp_ctx->name);
```

[↩ Reply](#) [↩↩ Reply All](#) [➡ Forward](#) [More ▾](#)

20/09/16 17:33

- Automate credentials pre-loading in RODC environments (add Administrator to RODC replication group + RODC preload run)
- Give a proper server for the referrals (PDC or replication partner instead of hardcoding)
- Add the same check in the deleted case

```
+ referral = calloc(sizeof(struct referral), 1);  
+ if (!referral) return -1;  
+ referral->url = strdup("ldap://gar-mas-0-0.%s/%s",  
+                        logfs_domainname(log_ctx),  
+                        logfs_name(log_ctx));
```

```
Hardware watchpoint 1: -location mRawPtr
Old value = (nsIContent *) 0x7feb51c3b900
New value = (nsIContent *) 0x7feb51c3b9c0
nsldapi_hex_unescape (s=0x7feb523cf3c6 "",
    s@entry=0x7feb523cf3a0 "gar-mas-0-0.", '\344' <repeats 14 times>, "\300\271\303Q\353\177\300\271\303Q\353\177")
    at /home/garming/comm-central/ldap/c-sdk/libraries/libldap/unescape.c:71
71         *p = '\0';
```

```
+         && !ldb_request_get_control(req, DSDB_CONTROL_DBCHECK_MODIFY_RO_REPLICA)) {
+     bool rodc = false;
+     struct loadparm_context *lp_ctx;
+     char *referral;
+
+     ret = samdb_rodc(ldb, &rodc);
+     if (ret != LDB_SUCCESS) {
+         DEBUG(4, (__location__ ": unable to tell if we are an RODC\n"));
+     } else if (rodc) {
+         ldb_set_errstring(ldb, "RODC modify is forbidden!");
+         lp_ctx = talloc_get_type(ldb_get_opaque(ldb, "loadparm"),
+                                 struct loadparm_context);
+
+         referral = talloc_asprintf(req,
+                                     "ldap://gar-mas-0-0.%s/%s",
+                                     lpcfg_dnsdomain(lp_ctx),
+                                     ldb_dn_get_linearized(req->op.add.message->dn));
+         ret = ldb_module_send_referral(req, referral);
+         return ret;
+     }
+ }
```

ldap/c-sdk/libraries/libldap/unescape.c

unescape.c deals with *percent encoding*
(a.k.a. *url encoding* or *RFC 1738 encoding*)

2 short functions



```
/* ***** BEGIN LICENSE BLOCK *****
 * Version: MPL 1.1/GPL 2.0/LGPL 2.1
 *
 * The contents of this file are subject to the Mozilla Public License Version
 * 1.1 (the "License"); you may not use this file except in compliance with
 * the License. You may obtain a copy of the License at
 * http://www.mozilla.org/MPL/
 *
 * Software distributed under the License is distributed on an "AS IS" basis,
 * WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License
 * for the specific language governing rights and limitations under the
 * License.
 *
 * The Original Code is Mozilla Communicator client code, released
 * March 31, 1998.
 *
 * The Initial Developer of the Original Code is
 * Netscape Communications Corporation.
 * Portions created by the Initial Developer are Copyright (C) 1998-1999
 * the Initial Developer. All Rights Reserved.
 *
 * Contributor(s):
 *
 * Alternatively, the contents of this file may be used under the terms of
 * either of the GNU General Public License Version 2 or later (the "GPL"),
 * or the GNU Lesser General Public License Version 2.1 or later (the "LGPL"),
 * in which case the provisions of the GPL or the LGPL are applicable instead
 * of those above. If you wish to allow use of your version of this file only
 * under the terms of either the GPL or the LGPL, and not to allow others to
 * use your version of this file under the terms of the MPL, indicate your
 * decision by deleting the provisions above and replace them with the notice
 * and other provisions required by the GPL or the LGPL. If you do not delete
 * the provisions above, a recipient may use your version of this file under
 * the terms of any one of the MPL, the GPL or the LGPL.
 *
 * ***** END LICENSE BLOCK ***** */

/*
 * LIBLDAP unescape.c -- LDAP URL un-escape routines
 * We also tolerate URLs that look like: <ldapurl> and <URL:ldapurl>
 */

#include "ldap-int.h"

static int unhex( char c );

void
nsldap_hex_unescape( char *s )
{
    /*
     * Remove URL hex escapes from s... done in place. The basic concept for
     * this routine is borrowed from the WWW library HTUnEscape() routine.
     */
    char      *p;

    for ( p = s; *p != '\0'; ++p ) {
        if ( *p == '%' ) {
            if ( ++p != '\0' ) {
                *p = unhex( *p ) << 4;
            }
            if ( ++p != '\0' ) {
                *p++ += unhex( *p );
            }
        } else {
            *p++ = *p;
        }
    }
    *p = '\0';
}

static int
unhex( char c )
{
    return( c >= '0' && c <= '9' ? c - '0'
           : c >= 'A' && c <= 'F' ? c - 'A' + 10
           : c - 'a' + 10 );
}
```

url encoding

A “%” character followed by 2 hexadecimal digits encodes the byte those digits refer to.

%2f /

%23 #

%20 <space>

%09 <tab>

%25 %

%4B K (*you don't usually do this for letters*)

decoding a single hexadecimal character

0		0
1		1
2		2
3		3
4		4
5		5
6		6
7		7
8		8
9		9
a	A	10
b	B	11
c	C	12
d	D	13
e	E	14
f	F	15

C means 12

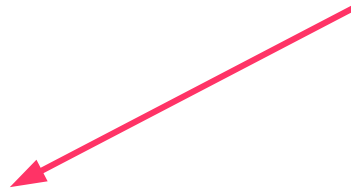
c also means 12

3 means 3

decoding a single hexadecimal character with unhex()

```
static int
unhex( char c )
{
    return( c >= '0' && c <= '9' ? c - '0'
           : c >= 'A' && c <= 'F' ? c - 'A' + 10
           : c - 'a' + 10 );
}
```

converting digits




... # \$ % ... / 0 1 2 3 4 5 6 7 8 9 : ... ? @ A B C D E F G ... _ ` a b c d e f g h ... r s t u ...

0 1 2 3 4 5 6 7 8 9

Decoding a single hexadecimal character with unhex()

```
static int
unhex( char c )
{
    return( c >= '0' && c <= '9' ? c - '0'
           : c >= 'A' && c <= 'F' ? c - 'A' + 10
           : c - 'a' + 10 );
}
```

converting A-F




... # \$ % ... / 0 1 2 3 4 5 6 7 8 9 : ... ? @ A B C D E F G ... _ ` a b c d e f g h ... r s t u ...

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Decoding a single hexadecimal character with unhex()

```
static int
unhex( char c )
{
    return( c >= '0' && c <= '9' ? c - '0'
           : c >= 'A' && c <= 'F' ? c - 'A' + 10
           : c - 'a' + 10 );
```



converting *a-f*

```
}
```

... # \$ % ... / 0 1 2 3 4 5 6 7 8 9 : ... ? @ A B C D E F G ... _ ` a b c d e f g h ... r s t u ...

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 10 11 12 13 14 15

Decoding a single hexadecimal character with unhex()

```
static int
unhex( char c )
{
    return( c >= '0' && c <= '9' ? c - '0'
           : c >= 'A' && c <= 'F' ? c - 'A' + 10
           : c - 'a' + 10 );
}
```

converting *a-f*

... and *g*

...	#	\$	%	...	/	0	1	2	3	4	5	6	7	8	9	:	...	?	@	A	B	C	D	E	F	G	...	_	`	a	b	c	d	e	f	g	h	...	r	s	t	u	...
						0	1	2	3	4	5	6	7	8	9					10	11	12	13	14	15							10	11	12	13	14	15	16					

Reading a single hex byte

```
static int
unhex( char c )
{
    return( c >= '0' && c <= '9' ? c - '0'
           : c >= 'A' && c <= 'F' ? c - 'A' + 10
           : c - 'a' + 10 );
}
```

converting a-f

... and everything else

... # \$ % ... / 0 1 2 3 4 5 6 7 8 9 : ... ? @ A B C D E F G ... _ ` a b c d e f g h ... r s t u ...

-52 -51 -50 ... -40 0 1 2 3 4 5 6 7 8 9 -29 ... -24 -23 10 11 12 13 14 15 -16 ... 8 9 10 11 12 13 14 15 16 17 ... 27 28 29 39 ...

```

void
nsldapi_hex_unescape( char *s )
{
    /*
     * Remove URL hex escapes from s... done in place.  The basic concept for
     * this routine is borrowed from the WWW library HTUnEscape() routine.
     */
    char    *p;

    for ( p = s; *s != '\0'; ++s ) {
        if ( *s == '%' ) {
            if ( *++s != '\0' ) {
                *p = unhex( *s ) << 4;
            }
            if ( *++s != '\0' ) {
                *p++ += unhex( *s );
            }
        } else {
            *p++ = *s;
        }
    }

    *p = '\0';
}

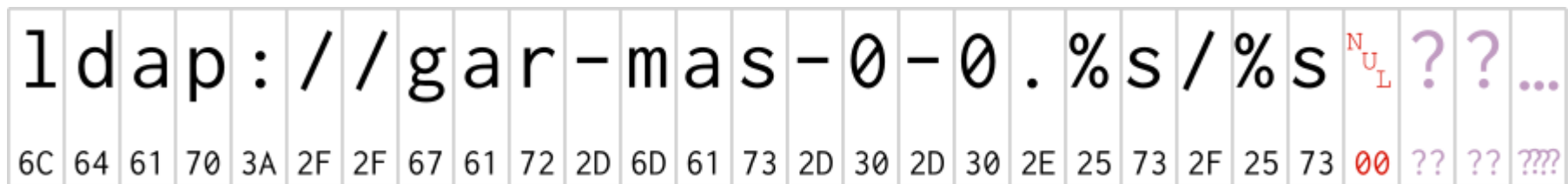
```

The string “*ldap://gar-mas-0-0.%s/%s*” in memory

C string handling:

A zero “nul” byte
ends the string

Memory beyond
the nul byte is
for something else



l	d	a	p	:	/	/	g	a	r	-	m	a	s	-	0	-	0	.	%	s	/	%	s	NUL	??	??	...
6C	64	61	70	3A	2F	2F	67	61	72	2D	6D	61	73	2D	30	2D	30	2E	25	73	2F	25	73	00	??	??	???

“ldap://gar-mas-0-0.%s/%s” after preprocessing

Ignore the
protocol part

The path is
broken into
separate strings

l	d	a	p	:	/	/	g	a	r	-	m	a	s	-	0	-	0	.	%	s	^N _U _L	%	s	^N _U _L	?	?	...
6C	64	61	70	3A	2F	2F	67	61	72	2D	6D	61	73	2D	30	2D	30	2E	25	73	00	25	73	00	??	??	???


```

for ( p = s; *s != '\0'; ++s ) {
    if ( *s == '%' ) {
        if ( *++s != '\0' ) {
            *p = unhex( *s ) << 4;
        }
        if ( *++s != '\0' ) {
            *p++ += unhex( *s );
        }
    } else {
        *p++ = *s;
    }
}

```

does *s* point to a percent?

no.

then copy it to *p*.
(and move *p* along).

```

*p = '\0';

```



l	d	a	p	:	/	/	g	a	r	-	m	a	s	-	0	-	0	.	%	s	^{NUL}	%	s	^{NUL}	?	?	...
6C	64	61	70	3A	2F	2F	67	61	72	2D	6D	61	73	2D	30	2D	30	2E	25	73	00	25	73	00	??	??	???

```

for ( p = s; *s != '\0'; ++s ) {
    if ( *s == '%' ) {
        if ( *++s != '\0' ) {
            *p = unhex( *s ) << 4;
        }
        if ( *++s != '\0' ) {
            *p++ += unhex( *s );
        }
    } else {
        *p++ = *s;
    }
}

```

then move s along

does s point to NUL?

no...

keep going

```
*p = '\0';
```



l	d	a	p	:	/	/	g	a	r	-	m	a	s	-	0	-	0	.	%	s	^{NUL}	%	s	^{NUL}	?	?	...
6C	64	61	70	3A	2F	2F	67	61	72	2D	6D	61	73	2D	30	2D	30	2E	25	73	00	25	73	00	??	??	???

```

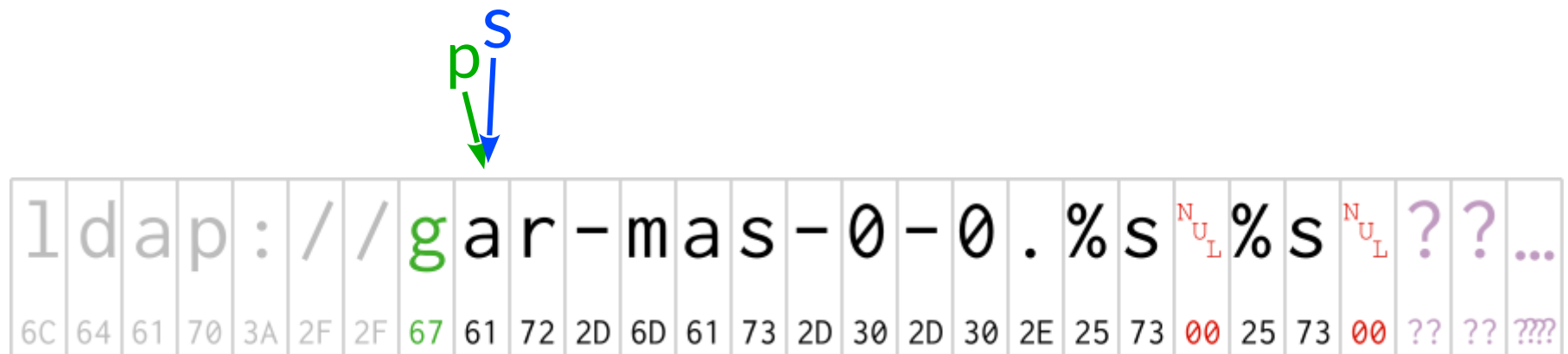
for ( p = s; *s != '\0'; ++s ) {
    if ( *s == '%' ) {
        if ( *++s != '\0' ) {
            *p = unhex( *s ) << 4;
        }
        if ( *++s != '\0' ) {
            *p++ += unhex( *s );
        }
    } else {
        *p++ = *s;
    }
}

```

```

*p = '\0';

```



```

for ( p = s; *s != '\0'; ++s ) {
    if ( *s == '%' ) {
        if ( *++s != '\0' ) {
            *p = unhex( *s ) << 4;
        }
        if ( *++s != '\0' ) {
            *p++ += unhex( *s );
        }
    } else {
        *p++ = *s;
    }
}

```

does s point to a percent?

YES.

```
*p = '\0';
```



l	d	a	p	:	/	/	g	a	r	-	m	a	s	-	0	-	0	.	%	s	^{NUL}	%	s	^{NUL}	?	?	...
6C	64	61	70	3A	2F	2F	67	61	72	2D	6D	61	73	2D	30	2D	30	2E	25	73	00	25	73	00	??	??	???

```

for ( p = s; *s != '\0'; ++s ) {
    if ( *s == '%' ) {
        if ( *++s != '\0' ) {
            *p = unhex( *s ) << 4;
        }
        if ( *++s != '\0' ) {
            *p++ += unhex( *s );
        }
    } else {
        *p++ = *s;
    }
}

```

move s along
does it point to NUL?

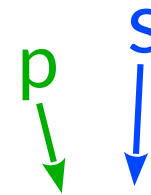
no...

then unhex it and write a
temporary value to p

```

*p = '\0';

```



l	d	a	p	:	/	/	g	a	r	-	m	a	s	-	0	-	0	.	?	s	^{NUL}	%	s	^{NUL}	?	?	...
6C	64	61	70	3A	2F	2F	67	61	72	2D	6D	61	73	2D	30	2D	30	2E	C0	73	00	25	73	00	??	??	???

```

for ( p = s; *s != '\0'; ++s ) {
    if ( *s == '%' ) {
        if ( *++s != '\0' ) {
            *p = unhex( *s ) << 4;
        }
        if ( *++s != '\0' ) {
            *p++ += unhex( *s );
        }
    } else {
        *p++ = *s;
    }
}

```

```

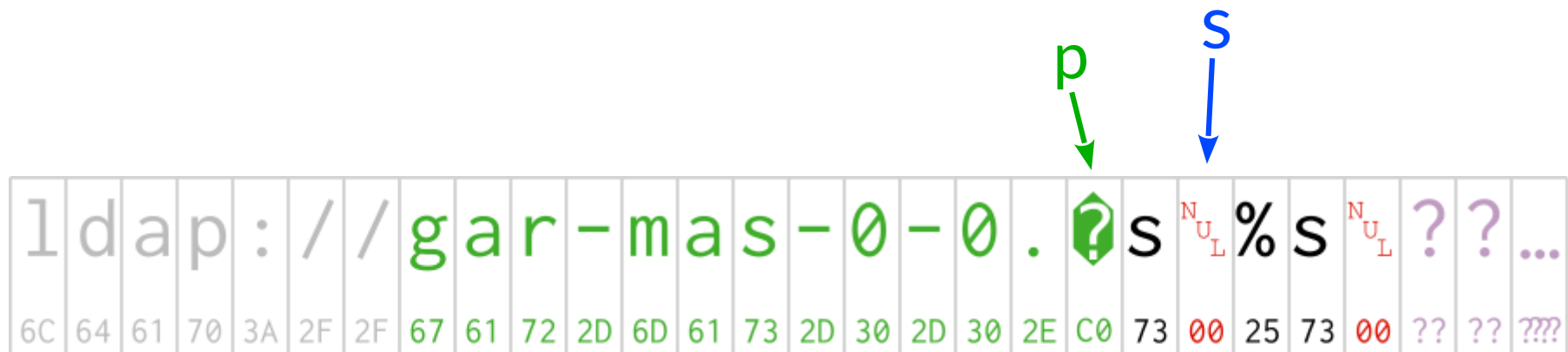
*p = '\0';

```

move s again
does it point to NUL now?

YES!

don't unhex it
don't move p on



```

for ( p = s; *s != '\0'; ++s ) {
    if ( *s == '%' ) {
        if ( *++s != '\0' ) {
            *p = unhex( *s ) << 4;
        }
        if ( *++s != '\0' ) {
            *p++ += unhex( *s );
        }
    } else {
        *p++ = *s;
    }
}

```

move s again
does it point to NUL now?

no

but it is another '%'

```

*p = '\0';

```



l	d	a	p	:	/	/	g	a	r	-	m	a	s	-	0	-	0	.	?	s	^{NUL}	%	s	^{NUL}	?	?	...
6C	64	61	70	3A	2F	2F	67	61	72	2D	6D	61	73	2D	30	2D	30	2E	C0	73	00	25	73	00	??	??	???

```

for ( p = s; *s != '\0'; ++s ) {
    if ( *s == '%' ) {
        if ( *++s != '\0' ) {
            *p = unhex( *s ) << 4;
        }
        if ( *++s != '\0' ) {
            *p++ += unhex( *s );
        }
    } else {
        *p++ = *s;
    }
}

```

repeat the “%s<sup>N_U_L” pattern
not moving *p*</sup>

```
*p = '\0';
```

p *s*

l	d	a	p	:	/	/	g	a	r	-	m	a	s	-	0	-	0	.	?	s	^{N_U_L}	%	s	^{N_U_L}	?	?	...
6C	64	61	70	3A	2F	2F	67	61	72	2D	6D	61	73	2D	30	2D	30	2E	C0	73	00	25	73	00	??	??	???


```

for ( p = s; *s != '\0'; ++s ) {
    if ( *s == '%' ) {
        if ( *++s != '\0' ) {
            *p = unhex( *s ) << 4;
        }
        if ( *++s != '\0' ) {
            *p++ += unhex( *s );
        }
    } else {
        *p++ = *s;
    }
}

```

```

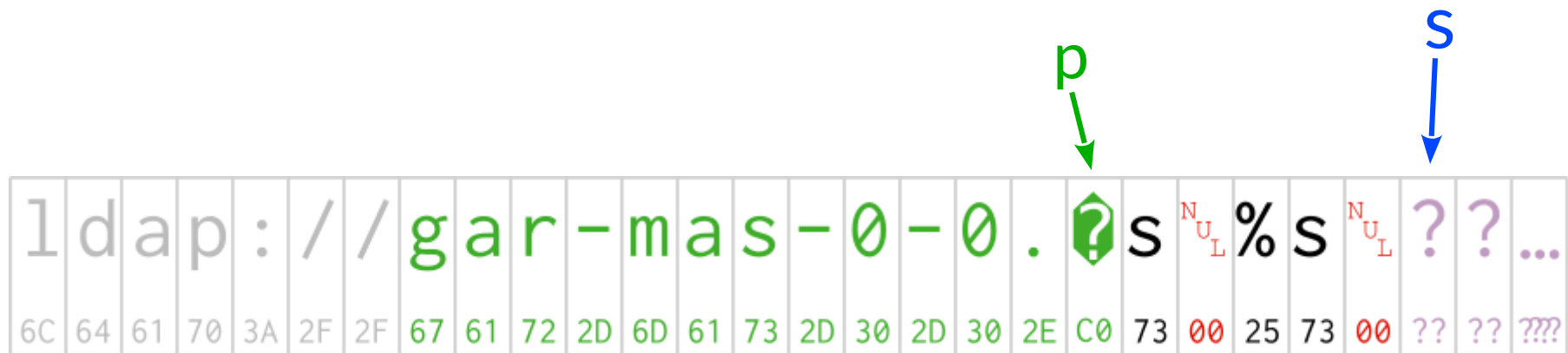
*p = '\0';

```

NOW does *s* point to NUL?

Nobody knows.

but if it doesn't,
the character is copied to *p*



```

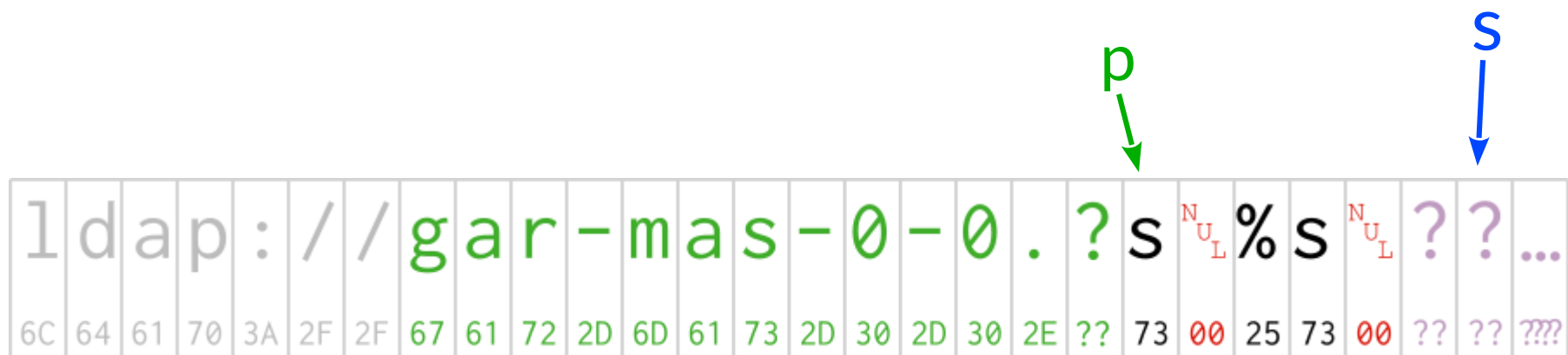
for ( p = s; *s != '\0'; ++s ) {
    if ( *s == '%' ) {
        if ( *++s != '\0' ) {
            *p = unhex( *s ) << 4;
        }
        if ( *++s != '\0' ) {
            *p++ += unhex( *s );
        }
    } else {
        *p++ = *s;
    }
}

```

```

*p = '\0';

```



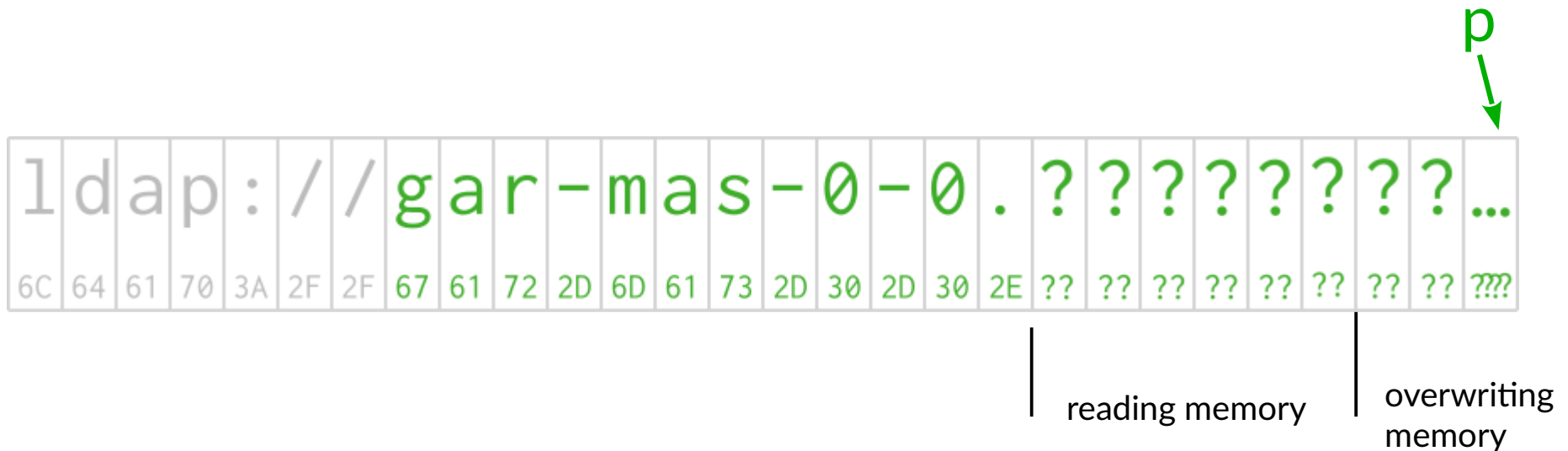
```

for ( p = s; *s != '\0'; ++s ) {
    if ( *s == '%' ) {
        if ( *++s != '\0' ) {
            *p = unhex( *s ) << 4;
        }
        if ( *++s != '\0' ) {
            *p++ += unhex( *s );
        }
    } else {
        *p++ = *s;
    }
}

```

Eventually s will hit a NUL and stop.

```
*p = '\0';
```

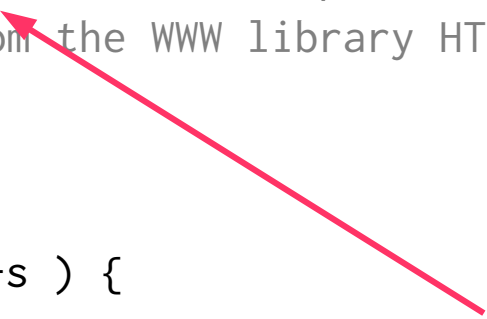


Who else is using this?

```
/*
 * Remove URL hex escapes from s... done in place. The basic concept for
 * this routine is borrowed from the WWW library HTUnEscape() routine.
 */
char    *p;

for ( p = s; *s != '\0'; ++s ) {
    if ( *s == '%' ) {
        if ( *++s != '\0' ) {
            *p = unhex( *s ) << 4;
        }
        if ( *++s != '\0' ) {
            *p++ += unhex( *s );
        }
    } else {
        *p++ = *s;
    }
}

*p = '\0';
}
```



Google for this string

[All](#)[Videos](#)[Images](#)[News](#)[Shopping](#)[More](#)[Settings](#)[Tools](#)

About 173 results (0.89 seconds)

[apr_ldap_url.c - \[svn.apache.org\]svn.us.apache.org; svn.eu.apache.org](#)https://svn.apache.org/repos/asf/apr/apr-util/tags/1.2.10/ldap/apr_ldap_url.c ▼

... static void apr_ldap_pvt_hex_unescape(char *s) { /* * **Remove URL hex escapes from s...** done in place. The basic concept for * this routine is borrowed from ...

[Copyright 2000-2004 The Apache Software Foundation * * Licensed ...](#)https://svn.apache.org/repos/asf/apr/apr-util/tags/1.0.0/ldap/apr_ldap_url.c

... static void apr_ldap_pvt_hex_unescape(char *s) { /* * **Remove URL hex escapes from s...** done in place. The basic concept for * this routine is borrowed from ...

[apr_ldap_url.c - The Apache Software Foundation!](#)https://svn.apache.org/repos/asf/apr/apr-util/branches/1.2.x/ldap/apr_ldap_url.c ▼

... static void apr_ldap_pvt_hex_unescape(char *s) { /* * **Remove URL hex escapes from s...** done in place. The basic concept for * this routine is borrowed from ...

[apr_ldap_url.c - The Apache Software Foundation!](#)https://svn.apache.org/repos/asf/apr/apr-util/branches/0.9.x/ldap/apr_ldap_url.c

NULL) { LDAP_VFREE(ludp->lud_exts); } LDAP_FREE(ludp); } static void
ldap_pvt_hex_unescape(char *s) { /* * **Remove URL hex escapes from s...** done in ...

[Apache/apr_ldap_url.c at master · omnigroup/Apache · GitHub](#)https://github.com/omnigroup/Apache/blob/master/apr-util/ldap/apr_ldap_url.c ▼

Remove URL hex escapes from s... done in place. The basic concept for. * this routine is borrowed from the WWW library HTUnEscape() routine. */. char *p;.

[illumos-nexenta/unescape.c at master · Nexenta/illumos-nexenta ...](#)<https://github.com/Nexenta/illumos-nexenta/blob/master/usr/src/lib/.../unescape.c> ▼

Remove URL hex escapes from s... done in place. The basic concept for. * this routine is borrowed from the WWW library HTUnEscape() routine. */. char *p;.



Search



Search

[Repositories](#) [Code](#)

553

[Commits](#) [Issues](#) [Wikis](#) [Users](#)

Languages

C

443

C++

2

Showing 448 available code results

Sort: **Best match** ▾[zheolong/melody-lib – unescape.c](#)

C

Showing the top three matches. Last indexed on 16 Sep 2016.

```
30  #include "ldap-int.h"
31
32
33  static int unhex( char c );
34
35
36  void
37  nsldapi_hex_unescape( char *s )
38  {
39  /*
40   * Remove URL hex escapes from s... done in place. The basic concept for
41   * this routine is borrowed from the WWW library HTUnEscape() routine.
```

[nxmirrors/onnv – unescape.c](#)

C

Showing the top three matches. Last indexed on 14 Sep 2016.

```
30  #include "ldap-int.h"
31
32
33  static int unhex( char c );
34
35
36  void
37  nsldapi_hex_unescape( char *s )
38  {
```

[Advanced search](#) [Cheat sheet](#)

233 files grepped (12 results)

Filter by package: [openldap](#), [389-dsgw](#), [icedove](#), [evolution](#), [evolution-data-server](#), [apr-util](#), [gnupg2](#) ▼☐ Group search results by Debian source package

All results

Pages: 1 2 >

[gnupg2_2.1.15-4/dirmngr/ldap-url.c](#)

```
{  
    /*  
        * Remove URL hex escapes from s... done in place. The basic concept for  
        * this routine is borrowed from the WWW library HTUnEscape() routine.  
        */
```

[gnupg2_2.1.18-6/dirmngr/ldap-url.c](#)

```
{  
    /*  
        * Remove URL hex escapes from s... done in place. The basic concept for  
        * this routine is borrowed from the WWW library HTUnEscape() routine.  
        */
```

[apr-util_1.5.4-3/ldap/apr_ldap_url.c](#)

```
{  
    /*  
        * Remove URL hex escapes from s... done in place. The basic concept for
```


Many of these have used openldap's version (fixed in 2002).

Most Github projects are dead forks.

Of the projects in Debian, only
icedove and *389-dsgw* have the bug.

Illumos (formerly Solaris) is also affected.

For a little while we thought we found a similar
problem in Firefox.

The fix

```
for ( p = s; *s != '\0'; ++s ) {  
    if ( *s == '%' ) {  
-        if ( *++s != '\0' ) {  
-            *p = unhex( *s ) << 4;  
+            if ( *++s == '\0' ) {  
+                break;  
            }  
-            if ( *++s != '\0' ) {  
-                *p++ += unhex( *s );  
+            *p = unhex( *s ) << 4;  
+            if ( *++s == '\0' ) {  
+                break;  
            }  
+            *p++ += unhex( *s );  
+  
        } else {  
            *p++ = *s;  
        }  
    }  
}
```

```

void
nsldapi_hex_unescape( char *s )
{
/*
 * Remove URL hex escapes from s... done in place. The basic concept for
 * this routine is borrowed from the WWW library HTUnEscape() routine.
 */
    char *p;

    for ( p = s; *s != '\0'; ++s ) {
        if ( *s == '%' ) {
            if ( *++s == '\0' ) {
                break;
            }
            *p = unhex( *s ) << 4;
            if ( *++s == '\0' ) {
                break;
            }
            *p++ += unhex( *s );

        } else {
            *p++ = *s;
        }
    }

    *p = '\0';
}

```

if you hit a NUL byte, **stop**

How can we call it a 25 year old bug when Thunderbird was first released in 2003?

Answer (part 1): the file is older

- * The Original Code is Mozilla Communicator client code, released
- * March 31, 1998.
- *
- * The Initial Developer of the Original Code is
- * Netscape Communications Corporation.
- * Portions created by the Initial Developer are Copyright (C) 1998-1999
- * the Initial Developer. All Rights Reserved.

and contains conflicting copyright claims:

- * Copyright (c) 1996 Regents of the University of Michigan.
- * All rights reserved.

Dates in other versions:

```
/* Copyright 2000-2005 The Apache Software Foundation or its licensors, as  
* applicable.
```

```
/* Portions Copyright 1998-2002 The OpenLDAP Foundation  
* All rights reserved.
```

```
* Portions Copyright (c) 1992-1996 Regents of the University of Michigan.  
* All rights reserved.
```

```
* Copyright (c) 1999 Apple Computer, Inc. All rights reserved.
```

It *probably* dates to around 1996

back to the source:

```
/*  
* Remove URL hex escapes from s... done in place. The basic concept for  
* this routine is borrowed from the WWW library HTUnEscape() routine.  
*/
```

HTUnEscape may skip over NUL byte...

- To: www-lib-bugs@w3.org
- Subject: HTUnEscape may skip over NUL byte...
- From: Markku Savela <msa@msa.tte.vtt.fi>
- Date: Thu, 14 Nov 1996 14:17:16 +0200 (EET)
- From www-lib-bugs-request@www10.w3.org Thu Nov 14 07:17:19 1996
- Message-Id: <199611141217.OAA16267@msa.tte.vtt.fi>
- Reply-to: msa@hemuli.tte.vtt.fi (Markku Savela)
- X-List-URL: <http://www.w3.org/pub/WWW/Archives/Public/www-lib-bugs/>

If HTUnEscape is given a string like "...%2", it will step over the terminating NUL byte, and with bad luck, if the next bytes are non-NUL, it may trash memory too. I think following minimal fix will repair the problem:

```
*** HTEscape.c.ORIG      Wed May  1 02:31:29 1996
--- HTEscape.c  Thu Nov 14 13:02:49 1996
*****
*** 112,119 ****
        if (*p == HEX_ESCAPE) {
            p++;
            if (*p) *q = from_hex(*p++) * 16;
!           if (*p) *q = FROMASCII(*q + from_hex(*p));
!           p++, q++;
        } else {
            *q++ = *p++;
        }
--- 112,119 ----
        if (*p == HEX_ESCAPE) {
            p++;
            if (*p) *q = from_hex(*p++) * 16;
!           if (*p) *q = FROMASCII(*q + from_hex(*p)), ++p;
!           q++;
        } else {
            *q++ = *p++;
        }
```

Disclaimer! This is of course my view of the matter. Someone in W3C should probably verify the patch (or invent a neater one).

three weeks later – fix as a compile-time option

Author: Eric Prud'hommeaux <eric@w3.org>
Date: Thu Dec 5 23:20:33 1996 +0000

goin' back to Cali

```
diff --git a/Library/src/HTEscape.c b/Library/src/HTEscape.c
index f83abea..6385928 100644
--- a/Library/src/HTEscape.c
+++ b/Library/src/HTEscape.c
@@ -112,8 +112,13 @@ PUBLIC char * HTUnEscape (char * str)
    if (*p == HEX_ESCAPE) {
        p++;
        if (*p) *q = from_hex(*p++) * 16;
+   #ifdef UNTESTED /* suggestion from Markku Savela - I just copied it in - EGP */
+       if (*p) *q = FROMASCII(*q + from_hex(*p)), ++p;
+       q++;
+   #else /* UNTESTED */
        if (*p) *q = FROMASCII(*q + from_hex(*p));
        p++, q++;
+   #endif /* !UNTESTED */
    } else {
        *q++ = *p++;
    }
}
```


18 months later

```
commit 0ccbc2c9fac13f7687e5cbe05ae11431b2ec89b2
Author: Henrik Frystyk Nielsen <frytstik@w3.org>
Date:   Fri Mar 20 17:53:18 1998 +0000
```

version 5.1k

```
diff --git a/Library/src/HTEscape.c b/Library/src/HTEscape.c
```

```
@@ -111,14 +110,15 @@ PUBLIC char * HTUnEscape (char * str)
    while(*p) {
        if (*p == HEX_ESCAPE) {
            p++;
-           if (*p) *q = from_hex(*p++) * 16;
-#ifdef UNTESTED /* suggestion from Markku Savela - I just copied it in - EGP */
-           if (*p) *q = FROMASCII(*q + from_hex(*p)), ++p;
+           if (*p) *q = HTAsciiHexToChar(*p++) * 16;
+#if 1
+           /* Suggestion from Markku Savela */
+           if (*p) *q = FROMASCII(*q + HTAsciiHexToChar(*p)), ++p;
            q++;
-#else /* UNTESTED */
-           if (*p) *q = FROMASCII(*q + from_hex(*p));
+#else
+           if (*p) *q = FROMASCII(*q + HTAsciiHexToChar(*p));
            p++, q++;
-#endif /* !UNTESTED */
+#endif
```

Actually only a 22 year old bug

Author: Henrik Frystyk Nielsen <frytstik@w3.org>
Date: Sun Nov 13 11:31:16 1994 +0000

Add HTEscape module

Trying to coordinate releases with the least possible effort

- get Illumos and Red Hat (389-dsgw) to sign up to Thunderbird bugzilla
- tell *them* to sort it out
- *[weeks pass; everyone waits]*
- Mozilla almost releases, others say no
- *[weeks pass]*
- Mozilla releases anyway

Garmin was awarded a bug bounty
but is ineligible because we are contractors.