

Re: [Full-disclosure] Gmail Oday

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2007-11/msg00255.html>

- *From:* "Adrian P" <unknown.pentester@xxxxxxxxxx>
 - *Date:* Sat, 10 Nov 2007 00:30:34 +0000
-

Hello Juergen,

With all my respect, is it that hard to see that gaining access to a Gmail session can lead to your identity being stolen?

Nowadays your webmail account means your online life/presence. Let's have a walk through attack shall we?

1. Your Gmail session is hijacked (i.e.: via the XSS PoC posted on FD)
2. Attacker searches for "password" in 'Inbox'/'Sent Mail'.
 - How many times have you clicked on "Forgot password" on MULTIPLE online accounts and the password (whether a new pass or the original one) emailed to you has not been changed from the time you got the "forgotten password" email?
 - How many users have emailed passwords to themselves so that they don't forget?
 - How many users use the same password on MULTIPLE online accounts (including merchant/e-commerce accounts)?
 - How many users have clicked on "remember credit card details" so that they don't have to re-enter their CC data every time they perform an online transaction?
 - Did you forget to disable your Gtalk chat history (Gtalk is still within the google.com domain)
 - Have you saved anything personal on other services such as Google docs/calendar/notebook? (or any other google.com service that doesn't require you to re-login once authenticated)
3. For most victims, this leads to a compromise of his/her online identity.

If you fail to see the problem, then please think before you complain about "damn, right now Oday are fucking XSS ...".

Re: [Full-disclosure] Gmail 0day

Posting a XSS PoC that opens an alert box doesn't have much merit perhaps. However, this is the equivalent of saying: "hey, I can cause a BO condition. If you send X parameter with 500 bytes/chars or more, then EIP is overwritten and the attacked service crashes". Now compare that to actually compromising the server via the buffer overflow vulnerability. That's a DIFFERENT STORY.

Same thing goes for any XSS. Now say, screw a cookie theft exploit for the Gmail XSS! (pardon my French). Make something more clever! Perhaps, you want a payload that scrapes all the victim's emails which contain keywords such as 'password', 'private', 'admin', and so on. Then, all the captured data is submitted to the attacker's site in the background (nothing suspicious is visually happening from the victim's point of view).

Sure Gmail has CSRF protection, but that can be bypassed via XSS. After all, anti-CSRF tokens can be grabbed if URLs can be accessed within the security context of the target domain (which is possible via XSS).

If you consider all the aforementioned thoughts plus the fact that Gmail is one of the most popular webmail services, then you should be able to understand the power of a XSS vul on google.com !

Regards,
AP.

On Nov 8, 2007 8:55 PM, Juergen Marester <marester.juergen@xxxxxxxx> wrote:

wow ! 0day !
damn, right now 0day are fucking XSS ...

On 11/8/07, silky <michaelslists@xxxxxxxx> wrote:

worked for me minutes after it was posted. seems fixed now.

On 11/9/07, crazy frog crazy frog <i.m.crazy.frog@xxxxxxxx> wrote:

i tested it on gmail latest version, itsnot working for me?

On Nov 8, 2007 7:04 AM, Scriptor Hack
<xss2root@xxxxxxxx > wrote:

There is a html injection vulnerability in
<https://www.google.com>.
It is very critical, you can get the cookie to
login into gmail ore

Re: [Full-disclosure] Gmail 0day

other

service.

POC:

<https://www.google.com/accounts/ServiceLogin?service=mail&rm=false&continue=http%3A%2F%2Fmail.g>

More:<http://xss2root.blogspot.com/>

Full-Disclosure – We believe in it.

Charter:

<http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia –

<http://secunia.com/>

==

advertise on secgeeks?

http://secgeeks.com/Advertising_on_Secgeeks.com

<http://newskicks.com>

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>

==

mike

<http://lets.coozi.com.au/>

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>

Re: [Full-disclosure] Gmail 0day

Re: [Full-disclosure] Gmail 0day

—
pagvac
gnucitizen.org, ikwt.com

Full-Disclosure – We believe in it.
Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>
Hosted and sponsored by Secunia – <http://secunia.com/>