

Forum: [Hack Forums](#)

Thread: [UNPATCHED GOOGLE VULNERABILITY \(RARE!!!\)](#)

Demoralise - April 2, 2016, 5:22 am

This is a reflected file download (RFD) vulnerability.

<http://www.google.com/finance/info:googlefinancepasswords.bat?q=ELI:ALTR&callback=gpedit.msc>

How to use:

- Only browser this works in that I know of is Firefox (most recent version) and IE < 11.
- Change googlefinancepasswords.bat to the desired batch file name.
- Change gpedit.msc to the desired cmd command.

You're welcome :)

Fleckens - April 2, 2016, 5:24 am

How can this be profitted? Let me know.

Zenfex - April 2, 2016, 9:05 am

Thank you very much, good sir :)

rezzex - April 2, 2016, 9:09 am

This actually works, tried with some Programs like notepad and all worked, the actually Program after it got opened gets a Error cause of wrong Arguments but it works :)

Evolved ® - April 2, 2016, 9:11 am

What can you do with this...?

Nuclear3mbargo - April 2, 2016, 12:38 pm

Here is a talk about RFD

<https://www.youtube.com/watch?v=dl1BJUNk8V4>

How to monetize? Using social engineering.

granz???????????????? - April 2, 2016, 2:23 pm

Yeah looks nice but hard to understand xD

ronald51 - April 3, 2016, 8:50 am

thanks a lot for this sharing, very handy.

ThaVinci - April 3, 2016, 12:06 pm

with bitsadmin command on Windows this works like a charm, google may fix this soon or I don't know, could be viral for ie and firefox users lol ;)

<http://pastebin.com/tYngjb7P>

Demoralise - April 9, 2016, 3:47 am

(Apr 3, 2016 12:06 PM)HandBrake Wrote: [\[CITE\]](#) with bitsadmin command on Windows this works like a charm, google may fix this soon or I don't know, could be viral for ie and firefox users lol ;)

<http://pastebin.com/tYngjb7P>Very good implementation!

gizmodo - April 9, 2016, 1:44 pm

thanks, for the info..will try this tonight.

?Syria - April 9, 2016, 2:03 pm

I have a question what will this do?

SIM-2212192 - April 9, 2016, 10:43 pm

Tried it on google chrome and microsoft edge, didn't seem to work on either, but maybe I'm just retarded.

Maybe it's only IE and FireFox like you said.):

DurkQ - April 10, 2016, 8:08 am

So, can I use this link to get my victim to download my RAT? Could someone please show me how...

LaiLaiZhen - April 10, 2016, 9:36 am

where is your payload hosted for this exploit?

denielsmith - April 23, 2016, 2:25 am

Thank you very much !!!!!

Demoralise - April 23, 2016, 2:26 am

(Apr 10, 2016 09:36 AM)LaiLaiZhen Wrote: [\[CITE\]](#) where is your payload hosted for this exploit?It isn't. It's a virtual download, an uploadless download.

Waterlemonanon - April 24, 2016, 4:16 am

Someone please explain what this is

3yZtwgIFSCUs - April 24, 2016, 4:23 am

awesome vulnerability hope somewhat amplication ddos with google ;)