

Forum:[Hack Forums](#)

Thread: [Sandboxie security flaws. \(Updated\)](#)

IcYSeptember - July 10, 2015, 8:08 pm

I'm using this old thread of mine to post this, instead of making a new one.

At the time of posting this thread, I did find another security flaw, though it was a local privilege escalation, which couldn't be performed inside of Sandboxie itself.

I did find a few other various bugs and fun stuff, albeit not security related.

I have recently found multiple flaws, ranging from sandbox escape, to denial of service.

I have successfully:

Disabled Sandboxie entirely, entirely from within SbIE itself.

Executed an executable of my choosing outside of the Sandbox, from inside, using multiple separate methods.

Escalated privileges from user to SYSTEM abusing a flaw directly related to Sandboxie.

These methods are a bit more complex than the last. All but the privilege escalation are only affecting systems above XP (unless Sandboxie doesn't support XP, I'm not sure).

I will be posting a video some time tomorrow, I want to put the bypass and privilege bugs together first. (Day 3, at 3:30 AM EST of no sleep, so yeah)

These exploits do not require administrative privileges like the last.

One of the escape bugs, however, due to how it works, can take upwards of 1.5 minutes to occur (you'll understand why, as with the last one, PoC sources [c++] will be released after they are fixed).

LogitechCamMan - July 11, 2015, 8:42 pm

I don't quite understand how you are finding these security hole within sandboxie.

'Cynical - July 11, 2015, 8:48 pm

You're original one was fucking genius... They hopefully give you a decent monetary prize for this one.. (\$100 maybe?)

Looking forward to seeing how you managed it this time.

E M I N e M - July 11, 2015, 8:56 pm

Posting to come back and see the video ;)

Trenchguns - July 11, 2015, 9:05 pm

(Jul 11, 2015 08:56 PM)E M I N e M Wrote: [\[CITE\]](#) Posting to come back and see the video ;)

Somebody took the words out of my mouth XD

I'm glad to see someone with brains who is actually white hat XD

Considering you could've sold this for quite a bit of money I'd imagine.

Scy7e - July 11, 2015, 9:07 pm

(Jul 11, 2015 08:48 PM)?Roku Wrote: [\[CITE\]](#) You're original one was fucking genius... They hopefully

give you a decent monetary prize for this one.. (\$100 maybe?)

Looking forward to seeing how you managed it this time.
How is \$100 a decent prize?

OneWorldOrder - July 11, 2015, 9:16 pm

You should implement it into a builder so malware coders can spread harder

'Cynical - July 11, 2015, 9:20 pm

(Jul 11, 2015 09:07 PM)Scy7e Wrote: [\[CITE\]](#) How is \$100 a decent prize?
Considering he only got a life time key last night, it's pretty decent.
Plus, Sandboxie isn't /that/ big of a company.

lcYSeptember - July 12, 2015, 3:07 am

I'd say there's a little more hooking going on than it thinks.

Dex? - July 12, 2015, 3:10 am

maybe you should actually do something with this one mr hacker

lcYSeptember - July 12, 2015, 8:56 am

This one (or rather, these, multiple) aren't really that big, I don't think.

I can successfully crash Sandboxie from within the Sandbox, fake messages, and I can successfully write a file anywhere on the disk (when running outside of Sandboxie, not in it), even if I'm running as a limited user.

If I make anything out of these (without finding anything further), it'll be a privilege escalation exploit via dll hijacking, or via a scheduled task setup to run with the highest rights (I do believe you can create scheduled tasks via writing a file in a subdir of system32, but I'm not sure).

I also found a way to use Sandboxie in a completely opposite way than what it was supposed to do. Sandboxie, from my analysis, actually uses only ring-3 hooks (sbiedll.dll), though I believe (I can't analyse the driver file with my tools, and CBA to download one that can analyse a 64-bit file; if anyone wants to send me the 32-bit driver file I'd love you forever) it's registering certain callbacks that are triggered when a file does something. Essentially a supported way of hooking things.

Edit: Sorry, I got literally 0 sleep last night. I meant to add, by meaning "use it in a completely opposite way that what it was supposed to," if you set it up (in)correctly, which you can do programmatically, you can theoretically use Sandboxie as a rootkit.

I'll make a PoC of that, if I get a VM handy.

lcYSeptember - September 5, 2015, 12:32 am

I've updated this thread with some info.

Tutelary - September 5, 2015, 9:06 am

Do you have plans to disclose all this to Sandboxie? You could get into their wall of fame (if they have one).

lcYSeptember - September 5, 2015, 9:12 am

(Sep 5, 2015 09:06 AM)Tutelary Wrote: [\[CITE\]](#) Do you have plans to disclose all this to Sandboxie? You could get into their wall of fame (if they have one).
Yes, I do.

The last bypass left me with a full version of their software. Honestly, I'd be happy with a hall-of-fame, or just a reference/whatever for school.