Microsoft Windows Image Rendering Memory Limit DoS Research

Luis Alberto Cortes Zavala
Security Consultant

- **Introduction**

We make the research about this send we found the following situation:

We prefer to call it as “Microsoft Windows Image Rendering Memory Limit DoS”, on our research we test the following OS:

- Microsoft Windows 2k (All Patches)
- Microsoft Windows XP (Without And with all patches, Including SP)

The first time I try to exploit this I found my windows advisement of “Virtual Memory is Full”, and then the OS Crashed, after some test I found that it depends of the amount of memory needed to render the image for windows crashes or not, as the same the amount of virtual memory that we use to have.

On Windows XP SP1, we found that when we run a image as the size of 9999x9999 windows stop it for some seconds then, it come back, I make the image grow, we found if more size, more type to get it back the OS is taken, and at the end of course windows just stop it to respond, it works in the same way on windows 2k, but when we try on windows XP SP2, we get a little surprise.

At the beginning I don’t think on test it under SP2, but one friend have the Service Pack installed and ask to him if let me do some test, when I run the Proof of Concept code, I found the pc were a little bit slow, but I resize the image on the code to 999999x999999, I already have test this on my machine and it come backs, when I open the image, systems get slow as usually, but after some seconds it get crash, after that I wait for a minute, and a “blue screen” appear, and the pc reboot itself, after turn it on, a classic pop up appears “The System has recovered from a error”, and I try to see dump file.

Some people don't get it the code works, really I don't know why every time I tested the code, it has works perfectly.

At the end we decide to publish this paper and the code we use to test. If someone found more on this issue, we will be glad to know.

- **POC**

```
<html>
<head>
<title>Windows Dos </title>
</head>
<body>
<img src="http://www.domain.com/images/image.jpg" width="999999" height="999999"><br>
</body>
</html>
```

Note: If you don't get system crash just use more SRC, to call more images on the same size or a little bit. Until you crash the system.

- **Conclusion**

Image rendering on windows, use a large amount of virtual memory, makes the system crash when is too big to be managed.

Luis Alberto Cortes Zavala
Luis.cortes@hypersec.co.uk
http://www.hypersec.co.uk