# Threat Research

## New IE Zero-Day Found in Watering Hole Attack

**November 09, 2013 | by Xiaobo Chen, Dan Caselden**

FireEye Labs has identified a new IE zero-day exploit hosted on a breached website based in the U.S. It's a brand new IE zero-day that compromises anyone visiting a malicious website; classic drive-by download attack. The exploit leverages a new information leakage vulnerability and an IE out-of-bounds memory access vulnerability to achieve code execution.

## Exploitation

The information leak uses a very interesting vulnerability to retrieve the timestamp from the PE headers of `msvcrt.dll`. The timestamp is sent back to the attacker's server to choose the exploit with an ROP chain specific to that version of `msvcrt.dll`. This vulnerability affects Windows XP with IE 8 and Windows 7 with IE 9.

The memory access vulnerability is designed to work on Windows XP with IE 7 and 8, and on Windows 7. The exploit targets the English version of Internet Explorer, but we believe the exploit can be easily changed to leverage other languages. Based on our analysis, this vulnerability affects IE 7, 8, 9, and 10. This actual attack of this memory access vulnerability can be mitigated by EMET per Microsoft's feedback.

## Shellcode

This exploit has a large multi-stage shellcode payload. Upon successful exploitation, it will launch `rundll32.exe` (with `CreateProcess`), and inject and execute its second stage (with `OpenProcess`, `VirtualAlloc`, `WriteProcessMemory`, and `CreateRemoteThread`). The second stage isn't written to a file as with most common shellcode, which usually downloads an executable and runs it from disk.

## Summary

In summary, this post was intended to serve as a warning to the generic public. We are collaborating with the Microsoft Security team on research activities.

We will continue to update this blog as new information about this threat is found. FireEye would like to acknowledge and thank iSIGHT Partners for their assistance in this research.

[Update 12-20-2013]: Microsoft release a security bulletin, assigned CVE-2013-3918 and CVE-2014-0266 to this issue.

PREVIOUS POST

NEXT POST



**Recent Posts**

**25 Mar 2020**
This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits >

**23 Mar 2020**
Monitoring ICS Cyber Operation Tools and Software Exploit Modules To Anticipate Future Threats >

**17 Mar 2020**
Six Facts about Address Space Layout Randomization on Windows >

**RSS FEED:**
STAY CONNECTED