the Availability Digest

www.availabilitydigest.com
@availabilitydig

# IE Exploit Allows Remote Code Execution

May 2014

Security firm FireEye has recently discovered a zero-day vulnerability in Microsoft's Internet Explorer web browser. A zero-day vulnerability is one in which the first attack is made before the developer has become aware of the vulnerability. As yet unnamed, the vulnerability was reported by both FireEye and Microsoft on April 26, 2014.

The vulnerability affects IE6 through IE11. This is significant because these browsers represent 55% of all browsers worldwide.

## What is the Vulnerability?

According to a Microsoft vulnerability disclosure,

> "The vulnerability is a remote code execution vulnerability. The vulnerability exists in the way that Internet Explorer accesses an object in memory that has been deleted or has not been properly allocated. The vulnerability may corrupt memory in a way that could allow an attacker to execute arbitrary code in the context of the current user within Internet Explorer. An attacker could host a specially crafted website that is designed to exploit this vulnerability through Internet Explorer and then convince a user to view the website."

The code details of the vulnerability are described in much more detail in FireEye's initial report.[1]

The vulnerability bypasses both the ASLR and DEP security protections in Windows. ASLR (address space layout randomization) protects against attacks due to buffer overflow. In order to prevent an attacker from reliably jumping to a particular exploited function in memory, ASLR involves randomly arranging the positions of key data areas of a program, including the base of the executable and the positions of the stack, heap, and libraries, in a process' address space.

Data Execution Prevention (DEP) is a security feature that marks areas of memory as either "executable" or "nonexecutable." It allows only data in an "executable" area to be run by programs, services, device drivers, etc.

The good news is that the attacks seen so far seem to have relied on exploiting IE 9, 10 and 11 using Adobe Flash as an attack vector. The bug is not in Flash, so there is nothing that Adobe can fix. It's just that by using specially crafted Flash files, attackers can prepare the contents of memory in order to make a successful attack possible. Therefore, if it is convenient, the vulnerability can be inhibited by simply disabling the Adobe Flash plug-in in the browser until a Microsoft fix is available.

[1] New Zero-Day Exploit targeting Internet Explorer Versions 9 through 11 identified in Targeted Attacks, *FireEye*; April 26, 2014. http://www.fireeye.com/blog/uncategorized/2014/04/new-zero-day-exploit-targeting-internet-explorer-versions-9-through-11-identified-in-targeted-attacks.html

## What Are the Risks?

Malicious websites can be crafted to take advantage of this vulnerability. The user would have to go to the website to be attacked, but this is typically accomplished be phishing emails sent by attackers.

In addition, websites that accept or host user-provided content or advertisements could unknowingly contain specially crafted code to exploit this vulnerability.

Given access to this vulnerability, an attacker can gain the same user rights as the current user. If the current user is logged on as an administrator, the attacker has complete control of the system. It can install and run programs; view, change or delete data; or create new user accounts with full user rights.

FireEye has identified an ongoing attack campaign that it has dubbed "Operation Clandestine Fox." This attack is aimed at U.S. military, government, energy, and financial institutions. Since this campaign is still being investigated, FireEye has released no further information on it.

Internet Explorer is unaffected by the vulnerability on Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2, all of which run by default in a restricted mode, Enhanced Security Protection.

## Mitigating the Risks

There are several ways that are being suggested to mitigate the risk of this vulnerability:

- Since attacks so far have used Adobe Flash as the attack vector, disable Adobe Flash in the IE browser.

- Switch to a different browser such as Google's Chrome or Mozilla's Firefox.

- Deploy the Enhanced Mitigation Experience Toolkit (EMET) version 4.1 or above. The U.S. Computer Emergency Readiness Team (CERT) recommends that EMET be enabled when possible.

- Set Internet and Local Intranet security settings to "High" to block ActiveX Controls and Active Scripting, adding sites you trust to the Internet Explorer Trusted Sites zone.

- Modify the access control list to be more restrictive.

- Enhanced Protected Mode in IE10 and above breaks the exploit.

- Microsoft has suggested that the VGX dynamic library, which is responsible for rendering the Vector Markup Language (VML), be disabled. FireEye has found this to be effective.

## What About XP?

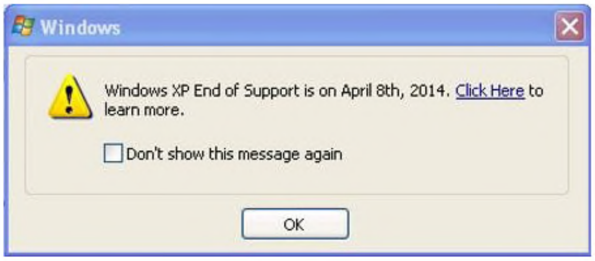
Unfortunately for XP users, Microsoft is sticking to its April 8, 2014 policy that upgrades to its thirteen-year old XP operating system will no longer be provided.[2] This presents a major problem because XP systems still represent about 25% of Windows installations worldwide.

[2] Windows XP Retirement a Boon for Hackers, *Availability Digest*; October 2013.
http://www.availabilitydigest.com/public_articles/0810/windows_xp.pdf

Microsoft has stated:

> “An unsupported version of Windows will no longer receive software updates from Windows Update. These include security updates that can help protect your PC from harmful viruses, spyware, and other malicious software, which can steal your personal information.”

Microsoft has been posting popups on Windows XP machines emphasizing this point, and it is encouraging users to upgrade to Windows 7 or 8 (this may require the purchase of a more powerful PC).



Windows XP End of Support is on April 8th, 2014. Click Here to learn more.

□ Don't show this message again

To make matters worse, FireEye has determined that “Operation Clandestine Fox” is attacking XP systems running IE7 and IE8 (IE8 is the last version of IE supported on XP).

Mitigation steps that can be taken by XP users include disabling the Adobe Flash browser plug-in. The VGX DLL can also be disabled by unregistering it using the following command-line sequence:

```
"%SystemRoot%\System32\regsvr32.exe" -u
"%CommonProgramFiles%\Microsoft Shared\VGX\vgx.dll"
```

## Summary

This zero-day vulnerability is still being actively exploited. Successful attackers can take over your system with your user privileges and can do arbitrary damage, especially if you are logged on as an administrator. Not only can the attacker steal or damage your data, but he can run arbitrary applications on your PC.

There are some straightforward steps that you can take to prevent attacks; and Microsoft, CERT, and the Department of Homeland Security suggest that you take action to protect your system as described above in the section entitled “Mitigating the Risks” until you have installed Microsoft’s corrective patch. If you are an XP user, there will be no corrective patch from Microsoft. Microsoft terminated support for XP on April 8, 2014.

## Acknowledgements

In addition to the references given above, material for this article was taken from the following sources:

Windows XP support has ended, *Microsoft*; April 8, 2014.
Vulnerability in Internet Explorer Could Allow Remote Code Execution, *Microsoft Security Advisory 2963983*; April 26, 2014.
Microsoft Races to Fix Massive Internet Explorer Hack: No Fix For Windows XP Leaves 1 In 4 PCs Exposed, *Forbes*; April 26, 2014.
Microsoft acknowledges “in the wild” Internet Explorer zero-day, *Naked Security*; April 27, 2014.
Microsoft confirms IE zero day being used in active exploits, *SearchSecurity*; April 28, 2014.
Microsoft rushes to fix browser after attacks: no fix for XP users, *Reuters*; April 29, 2014.
“Operation Clandestine Fox” Now Attacking Windows XP Using Recently Discovered IE Vulnerability, *FireEye*; May 1, 2014.