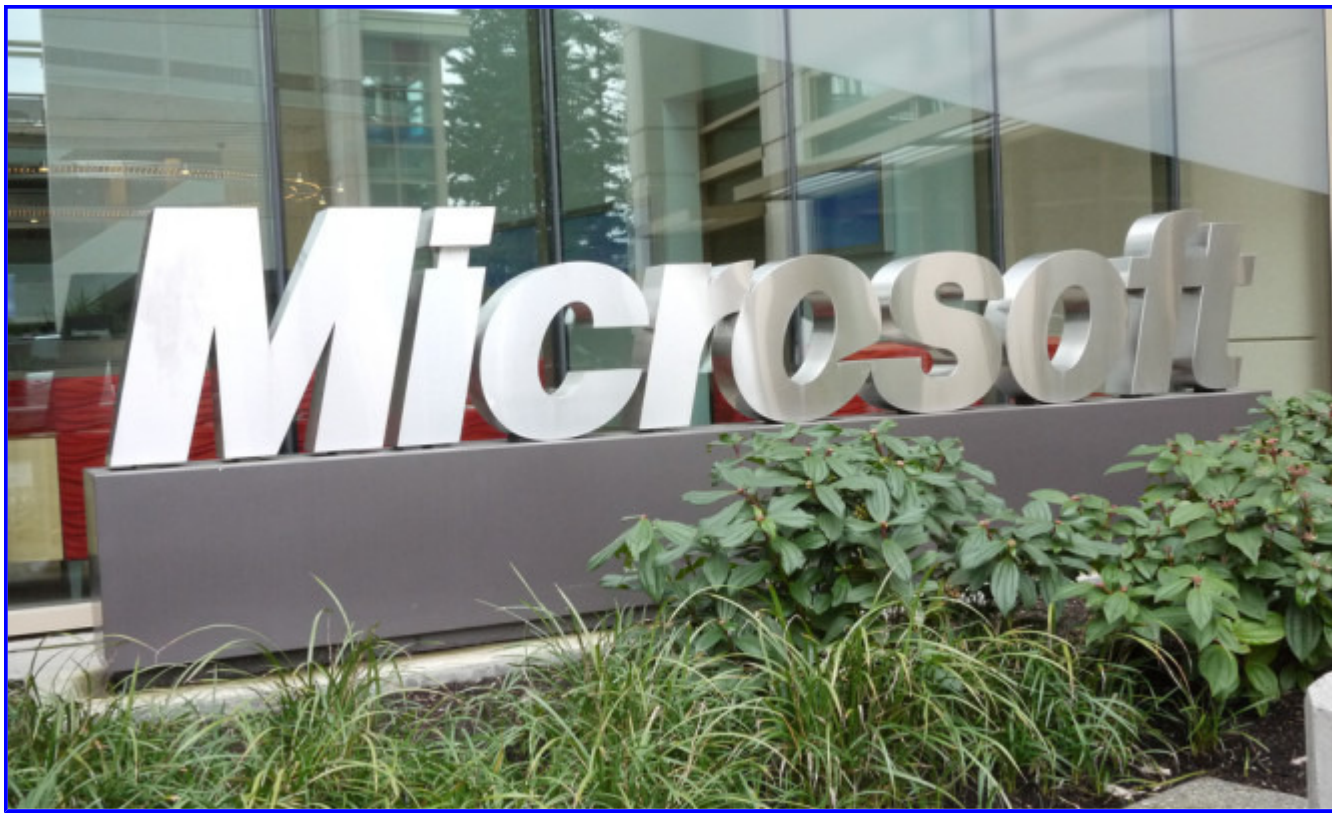

Microsoft Fixes ASLR/DEP Bypass Bug

Follow @dennisf by Dennis Fisher August 13, 2013 , 3:52 pm

Buried in the details of the Microsoft Patch Tuesday release for August is the explanation of an important change that the company made to Windows that defeats a group of exploit mitigation bypasses. The change is a small one, but it prevents dangerous attacks that previously worked on most supported version of Windows.

The last few versions of the operating system have included a portfolio of technologies known as exploit mitigations that are designed to prevent specific kinds of memory corruption attacks. These attacks rely on an underlying vulnerability, such as a buffer overflow, and often give the attacker control of a vulnerable machine. In the last several years, Microsoft has been adding more and more exploit mitigations to Internet Explorer and Windows both, and security researchers and attackers have been working apace to find ways around those defenses.

Related Posts

Microsoft Pulls Back Critical Exchange Server 2013 Patch

August 14, 2013 , 4:51 pm

Microsoft August Patch Tuesday Addresses Critical IE, Exchange and Windows Flaws

August 13, 2013 , 2:28 pm

Watering-Hole Attack Compromises Key Tibetan Site

August 12, 2013 , 2:35 pm

The two main exploit mitigations in Windows now are ASLR (Address Space Layout Randomization) and DEP (Data Execution Prevention). They're meant to defeat memory corruption attacks in most cases, and techniques that can bypass both of them are relatively rare and valuable. So much so, that Microsoft has started a bug bounty program that pays researchers up to $100,000 for techniques that can accomplish that feat. The technique that Microsoft fixed on Tuesday was demonstrated by a researcher at this year's CanSecWest conference, and likely would have qualified for that program, if it had existed at the time.

"The bypass takes advantage of a predictable memory region known as SharedUserData that exists at a fixed location (0x7ffe0000) in every process on every supported version of Windows. On 64-bit versions of Windows prior to Windows 8, this region contains pointers to multiple functions in the 32 -bit version of NTDLL that is used by WOW64 processes," Matt Miller and William Peteroy of Microsoft said in an analysis of the attack.

"The presence of these pointers at a predictable location in memory can enable an attacker to bypass ASLR if they have the ability to read anywhere in memory. In this case, the bypass technique takes things a step further by taking advantage of one of the functions listed above: LdrHotPatchRoutine. This function is part of the hotpatching support provided by Windows and one of the noteworthy things it does when called is load a DLL from a path that has been passed in as a field of the first parameter. This means that if an attacker can use a vulnerability to call LdrHotPatchRoutine, they could execute arbitrary code as a side effect of loading a malicious DLL of their choosing, such as from a UNC path, and thus bypass DEP implicitly.

"Depending on the vulnerability that is being exploited, it can be fairly straightforward for an attacker to trigger a call through the pointer to LdrHotPatchRoutine in SharedUserData with a controlled parameter, thus bypassing both ASLR and DEP."

The change that Microsoft made to address the problem is to eliminate the predictable pointer. This has the effect of not only defeating the existing, known attack technique, but also of mitigating similar attacks that might have taken advantage of another image pointer present in SharedUserData on 64-bit versions of Windows.

Image from Flickr photos of Bfishadow.

Categories: Microsoft

Leave A Comment

Your email address will not be published. Required fields are marked *