

[NT] Defeating Microsoft Windows XP SP2 Heap Protection and DEP Bypass

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0130.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/31/05

To: list@securiteam.com

Date: 31 Jan 2005 08:55:31 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Defeating Microsoft Windows XP SP2 Heap Protection and DEP Bypass

SUMMARY

The paper linked here suggest a method to defeat Windows XP SP2 heap protection, and bypassing DEP (Data Execution Prevention).

This technique was successfully tested by MaxPatrol team in trying to exploit the heap buffer overflow vulnerability in the Microsoft Windows winhlp32.exe application.

DETAILS

Overview:

Memory protection

Buffer overrun attacks are among the most common mechanisms, or vectors, for intrusion into computers. In this type of exploit, the attacker sends a long string to an input stream or control longer than the memory buffer allocated to hold it. The long string injects code into the system, which is executed, launching a virus or worm.

Windows XP Service Pack 2 uses two general categories of protection measures to inhibit buffer–overrun attacks. On CPUs that support it, the

Securiteam: [NT] Defeating Microsoft Windows XP SP2 Heap Protection and DEP Bypass

operating system can turn on the execution protection bit for virtual memory pages that are supposed to hold only data. On all CPUs, the operating system is now more careful to reduce both stack and heap buffer overruns, using "sandboxing" techniques.

Execution Protection (NX)

On the 64-bit AMD K8 and Intel Itanium processor families, the CPU hardware can mark memory with an attribute that indicates that code should not be executed from that memory. This execution protection (NX) feature functions on a per-virtual memory page basis, most often changing a bit in the page table entry to mark the memory page.

On these processors, Windows XP Service Pack 2 uses the execution protection feature to prevent the execution of code from data pages. When an attempt is made to run code from a marked data page, the processor hardware raises an exception immediately and prevents the code from executing. This prevents attackers from overrunning a data buffer with code and then executing the code; it would have stopped the Blaster worm dead in its tracks.

Although the support for this feature is currently limited to 64-bit processors, Microsoft expects future 32-bit and 64-bit processors to provide execution protection.

Sandboxing

To help control this type of attack on existing 32-bit processors, Service Pack 2 adds software checks to the two types of memory storage used by native code: the stack, and the heap. The stack is used for temporary local variables with short lifetimes; stack space is automatically allocated when a function is called and released when the function exits. The heap is used by programs to dynamically allocate and free memory blocks that may have longer lifetimes.

The protection added to these two kinds of memory structures is called sandboxing. To protect the stack, all binaries in the system have been recompiled using an option that enables stack buffer security checks. A few instructions added to the calling and return sequences for functions allow the runtime libraries to catch most stack buffer overruns. This is a case where a little paranoia goes a long way.

In addition, "cookies" have been added to the heap. These are special markers at the beginning and ends of allocated buffers, which the runtime libraries check as memory blocks are allocated and freed. If the cookies are found to be missing or inconsistent, the runtime libraries know that a heap buffer overrun has occurred, and raise a software exception.

Download Information:

The paper can be found at:

<<http://www.maxpatrol.com/defeating-xpsp2-heap-protection.pdf>>
<http://www.maxpatrol.com/defeating-xpsp2-heap-protection.pdf>

Securiteam: [NT] Defeating Microsoft Windows XP SP2 Heap Protection and DEP Bypass

Or in HTML format:

<<http://www.maxpatrol.com/defeating-xpsp2-heap-protection.htm>>
<http://www.maxpatrol.com/defeating-xpsp2-heap-protection.htm>

ADDITIONAL INFORMATION

The original article can be found at:

<<http://www.maxpatrol.com/defeating-xpsp2-heap-protection.htm>>
<http://www.maxpatrol.com/defeating-xpsp2-heap-protection.htm>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.