

[REVS] Defeating the Stack Based Buffer Overflow Prevention Mechanism of Microsoft Windows 2003 Server

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0036.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/14/03

To: list@securiteam.com

Date: 14 Sep 2003 19:11:47 +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 the Stack Based Buffer Overflow Prevention Mechanism of
Microsoft Windows 2003 Server

SUMMARY

This paper presents several methods of bypassing the protection mechanism built into Microsoft's Windows 2003 Server that attempts to prevent the exploitation of stack based buffer overflows. Recommendations about how to thwart these attacks are made where appropriate.

DETAILS

Introduction:

Microsoft is committed to security. David Litchfield has been playing with Microsoft products, as far as security is concerned, since 1997 and in the past year and a half or two David Litchfield has seen a marked difference with some very positive moves made. In a way, they had to. With the public relations crisis caused by worms such as Code Red Microsoft needed to do something to stem the flow of customers moving away from the Windows OS to other platforms. Microsoft's Trustworthy Computing push was born out of this and, in David's opinion, David Litchfield thinks we as consumers are beginning to see the results; or ironically not see them – as the holes

[REVS] Defeating the Stack Based Buffer Overflow Prevention Mechanism of Microsoft Windows 2003 Server

are just not appearing as they would if the security push was not there. We have, of course, seen at least one major security hole appear in Windows 2003 Server, this being the DCOM IRemoteActivation buffer overflow discovered by the Polish security research group, the Last Stages of Delirium <<http://www.lsd-pl.net>> <http://www.lsd-pl.net>. We will see more; but David Litchfield is confident that the number of security vulnerabilities that will be discovered in Windows 2003 Server will be a fraction of those found in Windows 2000. Acknowledging that there have been holes found and that, yes, more will come to light in the future this paper is going to look at how, currently, the stack based protection built into Windows 2003 Server to protect against buffer overflow vulnerability exploitation can be bypassed. The development of this mechanism is one of the right moves made in the direction of security.

An Overview of Windows 2003 Stack Protection:

Windows 2003 Server was designed to be secure out of the box. As part of the security in depth model adopted by Microsoft for their latest Windows version a new stack protection mechanism was incorporated into their compiler that was intended to help mitigate the risk posed by stack based buffer overflow vulnerabilities by attempting to prevent their exploitation. Technically similar to Crispin Cowan's StackGuard, the Microsoft mechanism places a security cookie (or canary) on the stack in front of the saved return address when a function is called. If a buffer local to that function is overflowed then, on the way to overwriting the saved return address, the cookie is also overwritten. Before the function, returns the cookie is checked against an authoritative version of the cookie stored in the .data section of the module where the function resides. If the cookies do not match then it is assumed that the buffer has been overflowed and the process is stopped. This security mechanism is provided by Visual Studio .NET – specifically the GS flag which is turned on by default. Currently the stack protection built into Windows 2003 can be defeated. David has engineered two similar methods that rely on structured exception handling that can be used generically to defeat stack protection. Other methods of defeating stack protection are available, but these are dependent upon the code of the vulnerable function and involve overwriting the parameters passed to the function.

ADDITIONAL INFORMATION

The complete article can be downloaded from:

<<http://www.nextgenss.com/papers/defeating-w2k3-stack-protection.pdf>>
<http://www.nextgenss.com/papers/defeating-w2k3-stack-protection.pdf>.

The information has been provided by <<mailto:nisr@nextgenss.com>>
NGSSoftware Insight Security Research.

=====

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.