

[REVS] Exploring Windows CE Shellcode

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0123.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/29/05

To: list@securiteam.com

Date: 29 Sep 2005 16:54:50 +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>

Exploring Windows CE Shellcode

SUMMARY

The linked paper discusses the problems involved in writing shellcode for Windows CE/ARM and goes on to develop an exploit. The full source for the exploit and related utilities is included.

DETAILS

Introduction:

Windows CE (WCE) is a Windows like operating system for various handheld devices, including Personal Digital Assistants (PDAs) and Mobile Phones. While at the API level, many of the function calls and interfaces are the same as the standard version of Windows, much of the internals have been altered to accommodate many different types of CPUs and architectures.

This paper will attempt to demonstrate the principals and techniques of exploiting WCE/ARM using an example vulnerability. Much of the information in this paper has been extracted from various public sources and in certain cases is used to exploit other architectures such as IA32.

It is assumed that the reader will have working knowledge of Windows exploit development and a grasp of the ARM assembly language. This knowledge is fundamental to some of the procedures and code in this paper.

ADDITIONAL INFORMATION

The information has been provided by <mailto:tim.hurman@pentest.co.uk>

Tim Hurman.

The original article can be found at:

<http://www.pentest.co.uk/documents/exploringwce/exploring_wce_shellcode.html>

http://www.pentest.co.uk/documents/exploringwce/exploring_wce_shellcode.html

=====

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.