

[NT] OllyDbg Format String Bug

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-07/0063.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/20/04

To: list@securiteam.com

Date: 20 Jul 2004 10:12:59 +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>

OllyDbg Format String Bug

SUMMARY

OllyDbg is a "32-bit assembler level analyzing debugger for Microsoft Windows". There exists a format string bug in the code that handles Debugger Messages in OllyDbg. This means any traced application can crash OllyDbg and execute machine code.

DETAILS

Vulnerable Systems:

* OllyDbg version 1.10

Typically OllyDbg attaches to a process and allows the user how to customize the session; whether they trace, or they breakpoint some stuff or whatever. The Windows API is actually very debugger friendly and has many functions to interact with debuggers (most likely built for their own (safe) debugger WinDbg). One of these functions, OutputDebugString sends a string directly to the debugger for interpretation, which OllyDbg displays to the user via a status line along the bottom, lacks a format specifiers, which means the user supplied string is used as the format specifiers.

To reproduce this excellent bug, these steps can be taken:

1. Download <<http://python.org>> Python and

Securiteam: [NT] OllyDbg Format String Bug

<<http://starship.python.net/crew/mhammond/win32/Downloads.html>> win32com.
These two are essential to any hacker's Windows box.

2. Run 'python' so you get an interactive shell.
3. Attach to the 'python' process with OllyDbg, press 'F9' to continue execution.
4. Type 'import win32api' and press enter in the python screen.
5. Type 'win32api.OutputDebugString("%s" * 50)' to crash OllyDbg. Typically, if you have OllyDbg set as the JIT Debugger, another OllyDbg screen will pop up OR
6. Type 'win32api.OutputDebugString("%8.8x" * 15)' to view what is currently in the stack
7. The python process will now have died since OllyDbg died, so do the process again

ADDITIONAL INFORMATION

The information has been provided by <<mailto:nd@felinemenace.org>> ned.

=====

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.