

[TOOL] Opcode Finder (In Memory)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0046.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/09/03

To: list@securiteam.com

Date: 9 Oct 2003 17:17:46 +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>

Opcode Finder (In Memory)

DETAILS

Opcode Finder is a Windows program that looks for certain x86 instructions (their opcodes) in any Win32 process' memory space. This can be later used in shellcode, JMP instructions, etc.

ADDITIONAL INFORMATION

The tool can be downloaded from: [<http://angelo.scanit.biz/>](http://angelo.scanit.biz/)
<http://angelo.scanit.biz/>.

The information has been provided by [<mailto:michael@scanit.be>](mailto:michael@scanit.be) Michael Hendrickx.

=====

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

=====
=====

Securiteam: [TOOL] Opcode Finder (In Memory)

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.