

[REVS] Win32 Message Vulnerabilities Redux

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0049.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 07/14/03

To: list@securiteam.com

Date: 14 Jul 2003 12:50:59 +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

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

Win32 Message Vulnerabilities Redux

SUMMARY

About one year ago, Chris Paget published a pair of papers that described fundamental flaws in the way the Microsoft Corp. Windows event model is designed. Paget showed how these flaws led to a class of attacks he dubbed "Shatter attacks", and claimed that they were both widespread and unfixable. The boldness of these claims led to a rash of media coverage of this exploit, and a sizeable debate within the security community about the accuracy and importance of his claims. In response to the pressure exerted by this attention, Microsoft published security bulletin MS02-071 and an associated patch, which has led many to believe that Shatter attacks are no longer possible.

DETAILS

iDEFENSE has published a paper written by Oliver Lavery that clarifies what the flaws in the Windows event model are, describes a related vulnerability that continues to exist in many popular software products and suggests ways in which these "unfixable" flaws might be addressed. Titled "Win32 Message Vulnerabilities Redux", the paper is available at

Securiteam: [REVS] Win32 Message Vulnerabilities Redux

<http://www.odefense.com/idpapers/Shatter_Redux.pdf>
http://www.odefense.com/idpapers/Shatter_Redux.pdf. The appropriate vendors mentioned within received an advance copy of this paper.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:listserv@odefense.com>>
iDEFENSE Labs.

=====

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.