

[NT] Microsoft Outlook mailto Command Line Switch Injection

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-03/msg00027.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 12 Mar 2008 09:13:48 +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>

Microsoft Outlook mailto Command Line Switch Injection

SUMMARY

<<http://office.microsoft.com/outlook/>> Microsoft Outlook provides "an integrated solution for managing and organizing e-mail messages, schedules, tasks, notes, contacts, and other information". Remote exploitation of an input validation error in the handling of "mailto" URIs by Microsoft Corp.'s Outlook may allow arbitrary code execution.

DETAILS

Vulnerable Systems:

- * Microsoft Outlook 2007 on Windows XP SP2

It is possible to construct a "mailto" URI which causes the web browser to pass extra command line switches to Outlook. These switches can modify Outlook's account configuration.

Analysis:

Exploitation of this vulnerability may allow an attacker to access sensitive information or take complete control of an affected system. In order to exploit this vulnerability, an attacker would have to convince a

[NT] Microsoft Outlook mailto Command Line Switch Injection

user to view an attacker-controlled website.

Workaround:

Disabling the "mailto" URI handler will prevent exploitation of this vulnerability. However, doing so will also disable e-mail links within all applications.

Vendor response:

Microsoft has addressed this vulnerability with Security Bulletin MS08-015. For more information, consult their bulletin at the following URL: <<http://www.microsoft.com/technet/security/Bulletin/ms08-015.mspx>>
<http://www.microsoft.com/technet/security/Bulletin/ms08-015.mspx>

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0110>>
CVE-2008-0110

Disclosure Timeline:

- 07/03/2007 – Initial vendor notification
- 07/03/2007 – Initial vendor response
- 03/11/2008 – Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by iDefense Labs.

The original article can be found at:

<<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=673>>
<http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=673>

=====

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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

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.