

[NT] Microsoft IE6 urlmon.dll Long URL Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-08/msg00100.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxx>
 - *Date:* 29 Aug 2006 15:10:59 +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>

Microsoft IE6 urlmon.dll Long URL Buffer Overflow

SUMMARY

NSFocus Security Team discovered a buffer overflow in IE 6.0SP1 which allows remote code execution via an over-long URL.

DETAILS

Security Bulletin MS06-042 released by Microsoft on August 8th, 2006 fixed multiple vulnerabilities, but the update for IE 6 introduced a new vulnerability.

When visiting websites with HTTP/1.1 protocol and data compression enabled, a buffer overflow might occur if an over-long URL is passed to IE 6. This overflow arises due to an incorrect call to function `lstrncpyA`, possibly resulting in heap data structure corruption. Carefully crafted data might lead to arbitrary code execution.

Attackers might craft a malicious WEB page and allure users to visit it in order to run arbitrary code with the users' privilege. If the user is the administrator, the attacker might gain complete control over the system. Attackers might host malicious web servers of their own, or exploit

[NT] Microsoft IE6 urlmon.dll Long URL Buffer Overflow

certain servers that enable HTTP/1.1 protocol and data compression in order to launch attacks.

Workaround:

Temporarily disable HTTP 1.1 support in IE.

Vendor Status:

2006.08.10 – Informed the vendor

2006.08.17 – Vendor confirmed the vulnerability

2006.08.24 – Microsoft released related patch and re-released MS06-042.

Detailed Microsoft Security Bulletin is available at:

<<http://www.microsoft.com/technet/security/bulletin/MS06-042.msp>>

<http://www.microsoft.com/technet/security/bulletin/MS06-042.msp>

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3869>>

CVE-2006-3869

ADDITIONAL INFORMATION

The information has been provided by <<mailto:security@xxxxxxxxxxxx>>
NSFOCUS Security Team.

The original article can be found at:

<<http://www.nsfocus.com/english/homepage/research/0608.htm>>

<http://www.nsfocus.com/english/homepage/research/0608.htm>

=====

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@xxxxxxxxxxxx

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

=====

=====

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.