

# [NT] Buffer Overflow in Internet Explorer's HTTP Parsing Code

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-04/0062.html>

---

*support\_at\_securiteam.com*

*Date:* 04/27/03

To: list@securiteam.com

Date: 27 Apr 2003 21:35:00 +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

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or [ussales@beyondsecurity.com](mailto:ussales@beyondsecurity.com)

-----

Buffer Overflow in Internet Explorer's HTTP Parsing Code

---

## SUMMARY

The code used in Microsoft Internet Explorer to parse web servers' HTTP replies contains a buffer overflow vulnerability. Specifically the faulty code is located in URLMON.DLL. A malicious user may exploit this vulnerability to execute arbitrary code on an IE user's system.

## DETAILS

HTTP is the protocol used in communication between web servers and web browsers. When a web page is viewed, the browser sends a HTTP request to the server in question. The server then sends a HTTP reply that usually contains the web page the browser requested. In addition to the document body that is shown to the user, the HTTP reply contains some header fields that e.g. specify how the document should be presented to the user.

Due to missing or insufficient input validation, a buffer overflow takes place in Internet Explorer when it receives a HTTP reply with excessively long values in certain header fields. A buffer placed on stack is overrun

## Securiteam: [NT] Buffer Overflow in Internet Explorer's HTTP Parsing Code

and a malicious reply may overwrite data, including the subroutine's return address, and thus direct the program execution to an arbitrary address. The vulnerability is a traditional stack-based buffer overflow and relatively easy to exploit.

This vulnerability can be used by an attacker to run any code in the system of the victim viewing a special web page with Internet Explorer or reading mail with Outlook or Outlook Express. More details will be published later.

### Solution:

The vendor was informed about the bug on March 16, 2003. Microsoft has classified this vulnerability as critical and published a bulletin and patch correcting the issue. These are available at <http://www.microsoft.com/technet/security/bulletin/MS03-015.asp>

The information in the "Mitigating factors" section of Microsoft's bulletin claiming that this vulnerability is not exploitable by e-mail borne attacks is incorrect. Test exploits have been produced for WWW, Outlook, and Outlook Express attack scenarios. In each of the cases, the exploit code runs without further user interaction on the victim system. Furthermore, no e-mail attachments or any kind of scripting are needed since the attack can be carried out via a standard HTML. In fact, merely starting the e-mail program can lead to exploitation because (depending on configuration) it may automatically open the first new message.

### ADDITIONAL INFORMATION

The information has been provided by <mailto:jouko@solutions.fi> Jouko Pynnonen.

=====

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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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.