

[NT] Microsoft IIS Vulnerable to Log Faking

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-11/0055.html>

From: support@securiteam.com

Date: 11/27/01

From: support@securiteam.com
To: list@securiteam.com
Subject: [NT] Microsoft IIS Vulnerable to Log Faking
Message-Id: <20011127072420.5B327138BF@mail.der-keiler.de>
Date: Tue, 27 Nov 2001 08:24:20 +0100 (CET)

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

When was the last time you checked your server's security?
How about a monthly report?
<http://www.AutomatedScanning.com> – Know that you're safe.

Microsoft IIS Vulnerable to Log Faking

SUMMARY

A security vulnerability in the way Microsoft's IIS logs incoming traffic allows attackers to fake log entries in the event log. The vulnerability is caused by the translation of incoming HEX replacements (%xx, where xx is an HEX code) into their original form, and the storage of its original form in the log file (for example %0A is translated into a new line). This vulnerability affects IIS in its default settings.

DETAILS

Log entries in the IIS log file have the hex codes in a request translated to a character.

For example /index%2easp becomes /index.asp and is stored in its translated form in the log file.

The problem rises from the fact that %0A is translated into a new line and %FF into what looks just like a space. Using these two, you can successfully create two perfectly real looking log entries.

Example:

/index.asp%FF200%FFHTTP/1.1%0A00:52:11%FF198.116.142.34%FFGET%FF/evilplaces

Securiteam: [NT] Microsoft IIS Vulnerable to Log Faking

Here the request for /index.asp is ended with a 200 notice and HTTP/1.1 showing what version has been used HTTP wise. Then a new line (%0A) is translated. Since all logging is done using Greenwich Time, all the attacker needs to do is figure out the current time in London and they are done. This is followed by the IP you want to 'frame', and then whatever you think they should be caught asking for.

The %FF and %0A works when using MS-DOS's Edit. To make this work in WordPad that more likely will be used to view logs, replace %FF with %09.

Final notes:

These days logs are used very often to prove illegal activity. When logs cannot be trusted there is a serious problem: how else do you prove illegal activity?

IIS 5.0 lets you set different logging formats. The example used the settings that were put there by the IIS installation (default installation). For us it was W3C Extended Log File Format, which logged the following things:

- Time (time)
- Client IP Address (c-ip)
- Method (cs-method)
- URI Stem (cs-uri-stem)
- Protocol Status (cs-status)
- Protocol Version (cs-version)

ADDITIONAL INFORMATION

The information has been provided by
<mailto:onesemicolon@onesemicolon.cjb.net> 1;.

=====

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.

-
- **Previous message:** support@securiteam.com: "[NEWS] A Cryptanalysis of the High-bandwidth Digital Content Protection System"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)