

# [NT] Microsoft IIS Logging Failure

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-01/0031.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 01/07/04

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 7 Jan 2004 18:07:34 +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 IIS Logging Failure

---

## SUMMARY

The HTTP protocol consists of requests and responses. Requests are sent from the clients (browsers) and they always start with a certain keyword (verb). The most common request is a "GET" request, but there are many more of these verbs, all of them are well documented within the RFCs. However, one of these verbs that Microsoft uses is not: it is the "TRACK" request. The TRACK request returns the original request as an entity (with a content-type of "message/http" and the returned body contains your original request), just like a TRACE request. The TRACE request is RFC compliant and well documented, the TRACK request is not RFC compliant and not documented (only one page mentions this verb in the MSDN library with no explanation). This request is not logged by the IIS server allowing attacks using this request to go unnoticed.

## DETAILS

Vulnerable systems:

- \* IIS version 5.0 and prior

Immune systems:

- \* IIS version 6.0

## Securiteam: [NT] Microsoft IIS Logging Failure

Making an HTTP request with the verb TRACK is not being logged. This makes it quite critical because it can be used to produce a lot of traffic and to get the 'Server' header and other valuable information. Furthermore, because the TRACK request is the same as a TRACE request, all known problems with TRACE requests also apply for this verb. The most important issue with a TRACE request is cross-site tracing (XST): a malicious web page or e-mail can send a TRACE/TRACK request to another website (by using client side scripting) and by analyzing the response it can have access to your credentials and your cookies on that site (think: session hijacking, passwords,...). All un-patched and future exploits that work with a TRACE request, should also work with the TRACK request but this time without being logged, making it ideal for probing vulnerable IIS systems.

### Exploit:

You can reproduce the problem using a tool like netcat and send the following line, followed by two CRLF pairs: TRACK / HTTP/1.0

You will see the response from IIS (just like a TRACE request), but you will not find this in the IIS log files.

### Vendor timeline:

2003.01.02 Found the vulnerability  
2003.05.29 Decided not to mail it to Microsoft  
2003.12.28 Released initial advisory

### ADDITIONAL INFORMATION

The original advisory is available at:

<<http://www.aqtronix.com/Advisories/AO-2003-02.txt>>  
<http://www.aqtronix.com/Advisories/AO-2003-02.txt>.

The information has been provided by <<mailto:parcifal@aqtronix.com>>  
Parcifal Aertssen.

=====

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.