

Securiteam: [NT] Windows Media Services Remote Command Execution (Large POST)

# [NT] Windows Media Services Remote Command Execution (Large POST)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-06/0097.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 06/26/03

To: list@securiteam.com

Date: 26 Jun 2003 18:18:29 +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

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at [canadasales@beyondsecurity.com](mailto:canadasales@beyondsecurity.com)

-----

Windows Media Services Remote Command Execution (Large POST)

---

## SUMMARY

As we reported in:

<<http://www.securiteam.com/windowsntfocus/5PP001FAAA.html>> Flaw in ISAPI

Extension for Windows Media Services Could Cause Code Execution, there is

a flaw in the way nsiislog.dll processes incoming client requests. A

vulnerability exists because an attacker could send specially formed HTTP

request (communications) to the server that could cause IIS to fail or

execute code on the user's system.

## DETAILS

Sending a large standard post to nsiislog.dll will cause an access

violation resulting in the following error log.

-----  
Event Type: Warning

Event Source: W3SVC

Securiteam: [NT] Windows Media Services Remote Command Execution (Large POST)

Event Category: None

Event ID: 37

Description:

Out of process application '/LM/W3SVC/1/Root' terminated unexpectedly.

-----  
This results in a standard stack based overflow, resulting in EIP been set to an arbitrary value allowing for remote command execution with privileges associated with the IWAM\_machinename account.

Example:

POST /scripts/nsiislog.dll HTTP/1.1

content-length: <postlength>

<post data>

Using Size: 4354

Connecting....Sending Buffer....

78028E9F mov al,byte ptr [esi] ESI = 00B138B4

Using Size: 5000

Connecting....Sending Buffer....

40F01F3B repne scas byte ptr [edi] EDI = 58585858

Using Size: 25000

Connecting....Sending Buffer....

78005994 mov dword ptr [edi],edx EDX = 58585858

-

58585858 ??? illegal op EIP = 58585858

Solution:

See the following article for a solution for this vulnerability:

<<http://www.securiteam.com/windowsntfocus/5PP001FAAA.html>>

<http://www.securiteam.com/windowsntfocus/5PP001FAAA.html>

ADDITIONAL INFORMATION

The information has been provided by

<mailto:brett.moore@security-assessment.com> Brett Moore.

=====

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

=====

=====

Securiteam: [NT] Windows Media Services Remote Command Execution (Large POST)

**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.