

## RE: Log Question

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2004-02/0063.html>

---

**From:** Davis, Matt ([matt.davis\\_at\\_countryfinancial.com](mailto:matt.davis_at_countryfinancial.com))

**Date:** 02/27/04

To: 'Sean Warnock ' <[swarnock@warnocksolutions.com](mailto:swarnock@warnocksolutions.com)>, "'focus-ms@securityfocus.com '" <[focus-ms@se](mailto:focus-ms@se)>  
Date: Fri, 27 Feb 2004 12:24:49 -0600

It looks like it is trying to exploit a buffer overflow in the Indexing Service... do a search for null.ida on google for more information. It exploits MS01-033...

HTH.

Matt Davis, MCSE: Security  
COUNTRY Insurance & Financial Services

-----Original Message-----

From: Sean Warnock  
To: [focus-ms@securityfocus.com](mailto:focus-ms@securityfocus.com)  
Sent: 2/27/04 10:54 AM  
Subject: Log Question

To all on the list;

Over the past few days I have been receiving a flurry of traffic on one of my web servers. I suspect it to be sometime of automated scan but I have been unable to find anything listed on Google with this type of signature. Fortunately whatever is going on is only getting a 404 error but I would like to learn a little more about what is going on. From what I can tell from reading so far it looks like a buffer overrun attempt on the indexing service. Below my signature you will find an excerpt from my log file. Any thoughts or insights would be appreciated.

Sean Warnock  
[swarnock@warnocksolutions.com](mailto:swarnock@warnocksolutions.com)

```
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2004-02-27 01:28:43
#Fields: date time c-ip cs-username s-ip s-port cs-method cs-uri-stem
cs-uri-query sc-status cs(User-Agent) cs(Referer)
2004-02-27 05:03:10 211.109.254.187 - 192.168.200.202 80 GET
/Default.htm - 200 - -
2004-02-27 05:03:10 211.109.254.187 - 192.168.200.202 80 GET /NULL.IDA
```

RE: Log Question



















