

# Re: Alert: Microsoft Security Bulletin – MS03–007

*Source:* <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-03/0036.html>

---

**From:** M. Burnett ([mb@XATO.NET](mailto:mb@XATO.NET))

**Date:** 03/17/03

Date: Mon, 17 Mar 2003 14:20:30 -0700  
From: "M. Burnett" <[mb@XATO.NET](mailto:mb@XATO.NET)>  
To: [NTBUGTRAO@LISTSERV.NTBUGTRAO.COM](mailto:NTBUGTRAO@LISTSERV.NTBUGTRAO.COM)

Just to clarify, Microsoft's bulletin states that this vulnerability could have been prevented using URLScan and/or IISLockdown, but it isn't really specific on how to do this. Several people have asked me how this can be done.

The following steps can be used to block the attack:

1. Completely disable WebDAV by setting the HKLM\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\DisableWebDAV registry key to 1
2. Limit the length of requests (the url and any headers) by setting the HKLM\SYSTEM\CurrentControlSet\Services\w3svc\parameters MaxClientRequestBuffer to something like 16k
3. Block the following WebDAV HTTP verbs using URLScan (either by specifically blocking them or by not listing them as allowed):  
OPTIONS, PROPFIND, PROPPATCH, MKCOL, DELETE, PUT, COPY, MOVE, LOCK, UNLOCK, OPTIONS, and SEARCH. Note that FrontPage does require the OPTIONS method to work properly.
4. Block the following WebDAV-related headers using the [DenyHeaders] section of URLScan.ini:  
[DenyHeaders]  
DAV:  
Depth:  
Destination:  
If:  
Label:  
Lock-Token:  
Overwrite:  
TimeOut:  
TimeType:  
DAVTimeOutVal:  
Other:

5. If you require WebDAV, you can limit the length of each individual header with these entries in the [RequestLimits] section (The exact values are obviously pretty generic and may need to be increased or decreased based on your particular configuration):

[RequestLimits]  
Max-DAV=250  
Max-Depth=250  
Max-Destination=250  
Max-If=250  
Max-Label=250  
Max-Lock-Token=250  
Max-Overwrite=250  
Max-TimeOut=250  
Max-TimeType=250  
Max-DAVTimeOutVal=250  
Max-Other=250

Microsoft does not specifically state which HTTP Verb and/or header is affected, but it does say that it is related to WebDAV. I would therefore assume that setting ACLs on httpext.dll would still be effective in blocking the attack. The PUT and DELETE methods are still available in IIS, but only as part of the original HTTP spec, not part of WebDAV.

Mark Burnett  
www.iisecurity.info

oo  
Delivery co-sponsored by TruSecure  
oo  
FREE WEBINAR: ICSA LABS' 2002 VIRUS PREVALENCE SURVEY RESULTS!

Join TruSecure and the ICSA Labs next Tuesday, March 18th, for our FREE webinar previewing the results of the ICSA Labs' 8th Annual Virus Prevalence Survey. Hear from the experts on the latest Internet attack trends, corporate security measures and virus/malware expectations for 2003, with recommendations on what you can do now to protect your organization. This webinar sells out every year, so click below to sign up today!

[www.trusecure.com/offer/s0080/](http://www.trusecure.com/offer/s0080/)

oo