

## Re: Article on WebDAV Vulnerability (MS03-007)

**Source:** <http://www.derkeiler.com/Newsgroups/comp.security.misc/2003-03/0603.html>

---

**From:** Karl Levinson [x y] mvp ([levinson\\_k@excite.com](mailto:levinson_k@excite.com))

**Date:** 03/24/03

From: "Karl Levinson [x y] mvp" <[levinson\\_k@excite.com](mailto:levinson_k@excite.com)>

Date: Mon, 24 Mar 2003 16:34:07 -0500

"aladin" <[aladin168@hotmail.com](mailto:aladin168@hotmail.com)> wrote in message  
news:bf0f8e77.0303240937.59259546@posting.google.com...  
> *KLC Consulting has published an article on the MS03-007 WebDAV  
> Vulnerability, which includes detection and mitigation  
> recommendations. This article consolidates many experts' inputs and  
> discussions. The URL is:  
> [http://www.klcconsulting.net/articles/webdav/webdav\\_vuln.htm](http://www.klcconsulting.net/articles/webdav/webdav_vuln.htm)*

Yes, yes, it's true that the patch is "the only way to be secure from this."  
However, IMHO some sources were too quick to remove and discount using  
URLScan and other tools IN ADDITION to the patch. The reason why the Army  
servers were hacked was they were relying on patches for security and not  
using URLScan, which would have prevented this compromise and other future  
IIS compromises. I hope those people got the message about the usefulness  
of ALSO using URLScan in addition to patching before the NTBugTraq FAQ on  
this was taken down.

The advice from Matt Scarborough stating that URLScan does not limit URL  
length AFAIK is not exactly correct. Nor is the advice from Microsoft to  
use the MaxURL setting in URLScan entirely correct. My understanding from  
the various Microsoft articles on URLScan is that the MaxURL setting was  
only introduced in URLScan 2.5 [which is not the version bundled with IIS  
Lockdown]. URLScan 2.1 also limits the MaxURL setting to a pretty small  
amount, but this is hard coded into the .DLL, not using the MaxURL setting.  
URLScan 2.0 and 1.0 may include this feature, but unfortunately there's no  
documentation from Microsoft to confirm this for you.

Personally if I was Microsoft, I might have included this information a  
little more prominently. The MS03-007 articles all simply state that  
"URLScan with the default settings will block this." Unfortunately, though,  
most people don't use the default settings.

RE: the reference to ISS for signatures to detect this exploit, ISS does not  
disclose their IDS signatures to anyone, not even their customers, much to  
the dismay of their customers. Also, I understand that ISS recently forced  
all their SiteProtector IDS customers to upgrade to the brand new

comp.security.misc: Re: Article on WebDAV Vulnerability (MS03-007)

SiteProtector 2.0 by immediately ceasing to produce new signatures for the previous version with zero overlap... even though it had just emerged from beta and still has bugs. I suppose their article is still useful for generally understanding this exploit, but unless I'm wrong, they're probably not ever going to be a useful place to get IDS signatures.