

SecurityFocus Microsoft: RE: code red----- on system that is already (and has been) patched

## RE: code red----- on system that is already (and has been) patched

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2003-03/0008.html>

---

*From:* Levinson, Karl ([LevinsonK@STARS-SMI.com](mailto:LevinsonK@STARS-SMI.com))

*Date:* 03/03/03

From: "Levinson, Karl" <[LevinsonK@STARS-SMI.com](mailto:LevinsonK@STARS-SMI.com)>

To: 'Sandy Ryan' <[sryan@seewolf.com](mailto:sryan@seewolf.com)>, [focus-ms@securityfocus.com](mailto:focus-ms@securityfocus.com)

Date: Mon, 3 Mar 2003 16:17:38 -0500

My understanding is that code 200 is exactly what you get in response to Code Red's GET /DEFAULT.IDA request, if you have installed the relevant security patch but have not yet removed the relevant script mappings from IIS. More information:

<http://securityadmin.info/faq.htm#iislogs2>

<http://securityadmin.info/faq.htm#iislogs>

Note that usually a HTTP code 200 is a disturbing code to see in the context of a worm, as it normally represents the successful execution of the attack command. In this case, however, the code 200 is inconclusive and does not in itself prove the success or failure of the attack. [Similarly, an HTTP 502 doesn't always prove that a particular attack failed.]

On the other hand, successful attacks from Nimda, Code Red, Sadmin, etc. will all show code 200's in the logs.

As your customer might already know, just installing patches does not by itself make your server secure. Your customer would want to consider also setting the correct settings, deleting the correct files, setting the appropriate file permissions, disabling services, etc. Installing patches may protect you from many of today's exploits, but not the exploits discovered tomorrow. The Baseline Security guidelines for Windows and IIS from [www.microsoft.com/technet/security](http://www.microsoft.com/technet/security) are one place to start, and/or the instructions at <http://securityadmin.info/faq.htm#harden>

HTH

– karl

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

From: Sandy Ryan [<mailto:sryan@seewolf.com>]

Sent: Monday, March 03, 2003 11:47 AM

To: [focus-ms@securityfocus.com](mailto:focus-ms@securityfocus.com)

Subject: [despammed] code red----- on system that is already (and has

RE: code red----- on system that is already (and has been) patched

SecurityFocus Microsoft: RE: code red----- on system that is already (and has been) patched  
been) patched

well – I doubt that the log is right – because I think the 200 implies  
that its not infected – by when my customer sees his report – and path  
taken through the site he sees worm.com

here's the log (simplified to get through the moderator)  
GET /default.ida

NN-----NN%u9090%u6858%ucbd3%u7801...%u9090%u9090%u8190%u00c3%u0003%u8b00%  
u531b%u53ff%u0078%u0000%u00=a 200 0 206 4039 266 HTTP/1.0 [you know the  
url]-- --