

Re: IIS : access to cmd.exe and multiple commands on one line

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-10/0170.html>

From: Garreth Jeremiah/Markham/IBM (gjeremia@ca.ibm.com)

Date: 10/24/01

Subject: Re: IIS : access to cmd.exe and multiple commands on one line
To: Emre Yildirim <emre@asper.org>
Message-ID: <OF6378F673.3BB918B8-ON85256AEF.004D8335@mkm.can.ibm.com>
From: "Garreth Jeremiah/Markham/IBM" <gjeremia@ca.ibm.com>
Date: Wed, 24 Oct 2001 10:01:14 -0400

I think that this has a lot to do with the various options supported by the cmd.exe executable under windows. Certain versions (notably those in WinNT and Win2K) have the ability to perform this function and is described in the HELP file for CMD.

the actual separators are probably affected by the parsing of IIS.....

===== Win23K cmd help =====

Note that multiple commands separated by the command separator '&&' are accepted for string if surrounded by quotes. Also, for compatibility reasons, /X is the same as /E:ON, /Y is the same as /E:OFF and /R is the same as /C. Any other switches are ignored.

If /C or /K is specified, then the remainder of the command line after the switch is processed as a command line, where the following logic is used to process quote (") characters:

1. If all of the following conditions are met, then quote characters on the command line are preserved:

- no /S switch
- exactly two quote characters
- no special characters between the two quote characters, where special is one of: &<>()@^|
- there are one or more whitespace characters between the two quote characters
- the string between the two quote characters is the name of an executable file.

2. Otherwise, old behavior is to see if the first character is a quote character and if so, strip the leading character and remove the last quote character on the command line, preserving any text after the last quote character.

SecurityFocus Penetration: Re: IIS : access to cmd.exe and mult

Garreth J Jeremiah.
CCSE,GCIA
IT Specialist (Security).
IBM Canada, SO Network Security.
(416) 657-2907
gjeremia@ca.ibm.com

Emre Yildirim
<emre@asper.or To: pen-test@securityfocus.com
> cc:
Subject: Re: IIS : access to cmd.exe and multiple commands on
10/23/2001 one line
06:12 PM
Please respond
to Emre
Yildirim

Alex Butcher (pentest) wrote:

>>*It is unclear to me whether this problem happens only because of the way
the
>>request is made (<http://path/to/cmd.exe?/c+command> or if
there are
>>really different versions of cmd.exe.*

This is probably unrelated to this thread but

After playing around with code red infected hosts, I found that
<http://path/to/cmd.exe?/rcommand+argument> works too. For example
<http://path/to/cmd.exe?/rdir+c:\> displays the contents of C:\.

Does anyone know what function the "r" plays in the URL?

--
Emre Yildirim <emre@asper.org>
PGP KeyID 0xF9E4A1D1 (keyserver.pgp.com)

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

Re: IIS : access to cmd.exe and multiple commands on one line

- *Previous message:* miguel.dilaj@pharma.novartis.com: "Re: IIS"
- *Maybe in reply to:* [Daniel Polombo: "IIS : access to cmd.exe and multiple commands on one line"](#)
- *Next in thread:* [Sam Steinmeyer: "RE: IIS : access to cmd.exe and multiple commands on one line"](#)
- *Messages sorted by:* [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)