

RE: [Full-Disclosure] Microsoft's Explorer and Internet Explorer long share name buffer overflow.

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-04/1086.html>

From: Bryce Porter (*bporter_at_heart.net*)

Date: 04/28/04

To: "KF (lists)" <kf_lists@secnetops.com>, <full-disclosure@lists.netsys.com>

Date: Wed, 28 Apr 2004 15:16:39 -0500

I tried this on Windows XP with SP1 on a few machines in my office, and had varying results.

If I went into the My Network Places, it recognized the 'share name' was too long and displayed an error dialog. It would not let me open the share and nothing else happened. Explorer did not lock up.

If I went Start -> Run -> \\server.ip.address, it immediately crashed explorer and asked the usual question 'Do you want to submit a bug report?'

I have not tried Internet Explorer yet, but I will keep you informed.

Regards,

Bryce Porter
Network Administrator
Heart Technologies, Inc.
Direct 309-634-2282
Fax 309-634-2382

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

From: KF (lists) [mailto:kf_lists@secnetops.com]

Sent: Monday, April 26, 2004 9:55 PM

To: full-disclosure@lists.netsys.com

Cc: bugtraq@securityfocus.com; submissions@packetstormsecurity.org; info@securiteam.com

Subject: Re: [Full-Disclosure] Microsoft's Explorer and Internet Explorer long share name buffer overflow.

This crashed IE 5.0.3700.1000 on Win2k SP4

Both the EBP and EIP were overwritten with 0x00410041.

ESP holds the Share name as passed by the server.

ESI holds servers.ip\sharename (tolowered)

I guess its unicode ninjitsu time.

-KF

Full-Disclosure: RE: [Full-Disclosure] Microsoft's Explorer and Internet Explorer long share name buffer overflow.

Milan 't4c' Berger wrote:

> *Hello,*
>
> *I experienced the same like Daniel.*
> *Windows 2k all hotfixes and patches installed.*
> *Machine doesn't crash, just gave me the error*
> *message "share name not found"*
>
> *Tested on german Windows 2000 pro SP4/IE6*
> *tested with Windows Explorer.*
>
>
> *Regards,*
> *Milan*
>
>
> *Daniel Regalado Arias wrote:*
>
>> *Well, i have tested it in W2k with sp3 and explorer*
>> *didnt get crashed!!!!!!*
>>
>> *Well, i cant get into the share because a message*
>> *appears saying "share name not found"!!!!*
>>
>> *But, explorer is OK.*
>>
>>
>> *--- Rodrigo Gutierrez <rodrigo@intellicomp.cl>*
>> *escribió: > Sunday afternoon is a bit boring, and*
>> *weather sucks*
>>
>>> *down here in Santiago,*
>>> *Chile so here we go...*
>>> *The vuln is attached in TXT format, I would be*
>>> *gratefull if someone could*
>>> *verify if it affects windows 2003 as well.*
>>>
>>> *Rodrigo.-*
>>>
>>>> *Microsoft Explorer and Internet Explorer Long*
>>>>
>>>
>> *Share*
>>
>>> *Name Buffer Overflow.*
>>>
>>>
>>>
>>> *Author: Rodrigo Gutierrez <rodrigo@intellicomp.cl>*
>>>

Full-Disclosure: RE: [Full-Disclosure] Microsoft's Explorer and Internet Explorer long share name buffer overflow.

>>> *Affected: MS Internet Explorer, MS Explorer*
>>> *(explorer.exe) Windows XP(All), Windows 2000(All)*
>>>
>>> *Not Tested: Windows 2003, Windows me, Windows 98,*
>>> *Windows 95*
>>>
>>> *Vendor Status: i notified the vendor in the*
>>> *beginning of 2002, this*
>>> *vulnerability was supposed to be*
>>> *fixed in xp service*
>>> *pack 1 according to the vendors*
>>> *knowledge base article*
>>> *322857.*
>>>
>>> *Vendor url:*
>>>
>>
>> <http://support.microsoft.com/default.aspx?scid=kb;en-us;322857>
>>
>>>
>>>
>>> *Background.*
>>>
>>> *MS Explorer (explorer.exe) and MS Internet*
>>> *Explorer(IEXPLORE.EXE) are core pieces of Microsoft Windows*
>>> *Operating Systems.*
>>>
>>>
>>>
>>> *Description*
>>>
>>> *Windows fails to handle long share names when*
>>> *accessing a remote file servers such as samba, allowing a malicious*
>>> *server to crash the clients explorer and eventually get to execute*
>>> *arbitrary code in the machine as the current user (usually with*
>>> *Administrator rights in windows*
>>> *machines).*
>>>
>>>
>>>
>>> *Analysis*
>>>
>>> *In order to exploit this, an attacker must be able*
>>> *to get a user to connect to a malicious server which contains a*
>>> *share name*
>>> *equal or longer than 300*
>>> *characters, windows wont allow you to create such a*
>>> *share, but of course samba includes the feature ;). After your*
>>> *samba box is*
>>> *up and running create a share in you smb.conf :*
>>>

Full-Disclosure: RE: [Full-Disclosure] Microsoft's Explorer and Internet Explorer long share name buffer overflow.

>>

>

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>