

Full-Disclosure: [Full-Disclosure] IIS double UTF decoding bug (old) exploit: IIS explorer

[Full-Disclosure] IIS double UTF decoding bug (old) exploit: IIS explorer

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2002-07/0014.html>

From: Steve (full-disclosure@lists.netsys.com)

Date: 07/11/02

From: full-disclosure@lists.netsys.com (Steve)

Date: Thu, 11 Jul 2002 12:26:56 -0400

On Thursday 11 July 2002 11:28 am, you wrote:

>(Ok, it's an old bug but since a lot of non-geeks seem to hate updating

> their IIS, there still are plenty of valid targets for this exploit.)

>

>-- SCRIPT KIDDIE COMPATIBLE EXPLOIT ATTACHED --

>The attached file IISexploere.php is my "SCRIPT KIDDIE COMPATIBLE" exploit

> for the double urldecoding bug in IIS. (It's a modified version of

> PHPexplorer, also written by yours truly ;)

<snip>

>Berend-Jan Wever aka SkyLined

><http://spoor12.edup.tudelft.nl>

>.

Since it looks like we are going to have tools to test holes, the policy of only releasing ones designing to test your own system for flaws, needs to be in. As Berend says we don't need to make it any easier for script kiddies.

Also, this list is going to have script kiddies on it so people needs to be kept aware of not posting specifics about their network which can then be used to root them. Too often I see people giving out all sorts of information about their network on lists thinking there are only white hats on it.

--

Steve Szmidt

V.P. Information Technology

Video Group Distributors, Inc.