

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/2002-07/0250.html>

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

Date: 07/11/02

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

Date: Thu, 11 Jul 2002 11:00:47 -0600

So how hard is it going to be to take a tool/script that only tests localhost and modify it to test other hosts? There is really no point in forcing localhost as it won't stop anyone.

Regards;

Steve Manzuik
Founder & Technical Lead
Entrench Technologies
www.entrenchtech.com

Moderator – VulnWatch
www.vulnwatch.org

www.csicon.net

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

From: "Steve" <steve@videogroup.com>

To: <full-disclosure@lists.netsys.com>

Sent: Thursday, July 11, 2002 10:26 AM

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

> *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*

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

> >.

>

> *Since it looks like we are going to have tools to test holes, the policy*

of

> *only releasing ones designed 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.*

>