

escalating IUSR to admin rights via unicode and iis4

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2002-07/0045.html>

From: ewwtwvi@hushmail.com

Date: 07/09/02

From: ewwtwvi@hushmail.com

To: pen-test@securityfocus.com

Date: Tue, 9 Jul 2002 10:18:15 -0700

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Hello,

I understand that this topic has been discussed in great deal, however i searched the archives and was unable to find anything.

In doing a security assessment – I came across a web server running iis4 that is vulnerable to the unicode exploit. I was able to get it to tftp back to my tftp server and pull down nc and a few other things...then got nc listening with a shell and was able to connect to that shell...I didnt go any further and reported it as it was. I was then questioned on the possibility of it being used to escalate rights to administrator..and asked for a demo... i repeated the above steps, but was unable to stop services and such. I couldnt even delete a file I had uploaded using unicode with tftp.

Could someone please point me to info that would explain what i have to do to accomplish this. I have been searching...but apparently not well enough.

Again, I hope this gets through..As it has proly been discussed very much. I apologize in advance for this question.. but im stuck :(

Thanks much!

t

-----BEGIN PGP SIGNATURE-----

Version: Hush 2.1

Note: This signature can be verified at <https://www.hushtools.com>

wlwEARECABwFAj0rGdkVHGV3dnR3dmlAaHVzaG1haWwuY29tAAoJEONDjIN5eMWV4yoA
n1TdHllf1vT//ZWzA/D9CaPaVC7bAKCyKMk5UUB8wzny2LtRDKWQNepzFw==
=yH9p

-----END PGP SIGNATURE-----

Communicate in total privacy.

Get your free encrypted email at <https://www.hushmail.com/?l=2>

SecurityFocus Penetration: escalating IUSR to admin rights via unicode and iis4

Looking for a good deal on a domain name? <http://www.hush.com/partners/offers.cgi?id=domainpeople>

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/>

- **Previous message:** [Jeremy Junginger: "Thoughts on VNC access?"](#)
- **Next in thread:** [Jeanette LaRosa: "Re: escalating IUSR to admin rights via unicode and iis4"](#)
- **Reply:** [Jeanette LaRosa: "Re: escalating IUSR to admin rights via unicode and iis4"](#)
- **Reply:** [juan.francisco.falcon@ar.pwcglobal.com: "Re: escalating IUSR to admin rights via unicode and iis4"](#)
- **Reply:** [Bill Pennington: "Re: escalating IUSR to admin rights via unicode and iis4"](#)
- **Reply:** [French, Dave: "RE: escalating IUSR to admin rights via unicode and iis4"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)