

Re: [Full-disclosure] Re: It's not that simple...

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-08/0577.html>

From: yossarian (yossarian_at_planet.nl)

Date: 08/18/05

Date: Thu, 18 Aug 2005 01:02:02 +0200

To: jasonc@science.org

In the original X-Force paper named pipes were mentioned besides Null Sessions. Does it need both or either one – the paper isn't clear on this? The named pipes seem to have dropped from all discussion.... Anyway, never broke anything by disabling them, either. This is a registry hack described in the MS Hardening guides for 2000 and 2003 server. Just like Null sessions. Elsewhere dunno, but probably, never bothered.

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

From: "Jason Coombs" <jasonc@science.org>

To: "Kurt Seifried" <listuser@seifried.org>

Cc: <full-disclosure@lists.grok.org.uk>

Sent: Thursday, August 18, 2005 12:24 AM

Subject: Re: [Full-disclosure] Re: It's not that simple...

> *Kurt Seifried wrote:*

>> *Actually it really is that simple. Disabling Null sessions is entirely possible, quite easy, and doesn't break a lot (at least in my previous*

>

> *Then why doesn't Microsoft provide these instructions in the workarounds section of the vulnerability announcement? Are you certain, Kurt, that the proposed registry hack is sufficient to prevent PnP null sessions? Perhaps they branch differently in the Windows 2000 code base.*

>

> <http://www.microsoft.com/technet/security/bulletin/MS05-039.mspx>

>

> *Workarounds for Plug and Play Vulnerability – CAN-2005-1983:*

>

> *Microsoft has tested the following workarounds. While these workarounds will not correct the underlying vulnerability, they help block known attack vectors. When a workaround reduces functionality, it is identified in the following section.*

>

> *Note Other protocols, such as Internetwork Packet Exchange (IPX) and Sequenced Packet Exchange (SPX), could be vulnerable to this issue. If you are using vulnerable protocols such as IPX and SPX, you should block the appropriate ports for those protocols. For more information about IPX and SPX, visit the following Microsoft Web site.*

Full-Disclosure: Re: [Full-disclosure] Re: It's not that simple...

- >
- > *Note As mentioned in the “Mitigating Factors” section, Windows XP Service*
- > *Pack 2 and Windows Server 2003 are vulnerable to this issue primarily from*
- > *locally logged on users. The following workarounds are designed primarily*
- > *for earlier operating system versions that are vulnerable to anonymous*
- > *network-based attacks.*
- > •
- > *Block TCP ports 139 and 445 at the firewall:*
- >
- > *These ports are used to initiate a connection with the affected protocol.*
- > *Blocking them at the firewall, both inbound and outbound, will help*
- > *prevent systems that are behind that firewall from attempts to exploit*
- > *this vulnerability. We recommend that you block all unsolicited inbound*
- > *communication from the Internet to help prevent attacks that may use other*
- > *ports. For more information about ports, visit the following Web site.*
- > •
- > *To help protect from network-based attempts to exploit this vulnerability,*
- > *use a personal firewall, such as the Internet Connection Firewall, which*
- > *is included with Windows XP Service Pack 1.*
- >
- > *By default, the Internet Connection Firewall feature in Windows XP Service*
- > *Pack 1 helps protect your Internet connection by blocking unsolicited*
- > *incoming traffic. We recommend that you block all unsolicited incoming*
- > *communication from the Internet.*
- >
- > *To enable the Internet Connection Firewall feature by using the Network*
- > *Setup Wizard, follow these steps:*
- >
- > 1.
- >
- >
- > *Click Start, and then click Control Panel.*
- >
- > 2.
- >
- >
- > *In the default Category View, click Network and Internet Connections, and*
- > *then click Setup or change your home or small office network. The Internet*
- > *Connection Firewall feature is enabled when you select a configuration in*
- > *the Network Setup Wizard that indicates that your system is connected*
- > *directly to the Internet.*
- >
- > *To configure Internet Connection Firewall manually for a connection,*
- > *follow these steps:*
- >
- > 1.
- >
- >
- > *Click Start, and then click Control Panel.*
- >
- > 2.

Full-Disclosure: Re: [Full-disclosure] Re: It's not that simple...

- >
- >
- > *In the default Category View, click Networking and Internet Connections,*
- > *and then click Network Connections.*
- >
- > 3.
- >
- >
- > *Right-click the connection on which you want to enable Internet Connection*
- > *Firewall, and then click Properties.*
- >
- > 4.
- >
- >
- > *Click the Advanced tab.*
- >
- > 5.
- >
- >
- > *Click to select the Protect my computer or network by limiting or*
- > *preventing access to this computer from the Internet check box, and then*
- > *click OK.*
- >
- > *Note If you want to enable certain programs and services to communicate*
- > *through the firewall, click Settings on the Advanced tab, and then select*
- > *the programs, the protocols, and the services that are required.*
- > •
- > *To help protect from network-based attempts to exploit this vulnerability,*
- > *enable advanced TCP/IP filtering on systems that support this feature.*
- >
- > *You can enable advanced TCP/IP filtering to block all unsolicited inbound*
- > *traffic. For more information about how to configure TCP/IP filtering, see*
- > *Microsoft Knowledge Base Article 309798.*
- > •
- > *To help protect from network-based attempts to exploit this vulnerability,*
- > *block the affected ports by using IPsec on the affected systems.*
- >
- > *Use Internet Protocol security (IPsec) to help protect network*
- > *communications. Detailed information about IPsec and about how to apply*
- > *filters is available in Microsoft Knowledge Base Article 313190 and*
- > *Microsoft Knowledge Base Article 813878.*
- >
- > _____
- > *Full-Disclosure – We believe in it.*
- > *Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>*
- > *Hosted and sponsored by Secunia – <http://secunia.com/>*

Full-Disclosure – We believe in it.
Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>
Hosted and sponsored by Secunia – <http://secunia.com/>