

RE: Secure Ldap call not working due to IUSR/IWAM permissions?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2003-02/0022.html>

From: Turner, Keith (Contractor) (Keith.Turner@tea.army.mil)

Date: 02/05/03

From: "Turner, Keith (Contractor)" <Keith.Turner@tea.army.mil>

To: 'Tony Gordon' <tony.gordon@hewitt.com>

Date: Wed, 5 Feb 2003 13:44:56 -0500

Thanks Tony! That hotfix did the trick.

I'm assuming that some of the settings I changed before installing sp3 is what lead to this problem. I have other machines I have configured the same way, but they were postsp3 – so the configuration changes were done after sp3 was installed.

Keith

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

From: Tony Gordon [<mailto:tony.gordon@hewitt.com>]

Sent: Monday, February 03, 2003 5:32 PM

To: Turner, Keith (Contractor)

Cc: focus-ms@securityfocus.com

Subject: Re: Secure Ldap call not working due to IUSR/IWAM permissions?

If this is W2K with SP3 take a look at

<http://support.microsoft.com/default.aspx?scid=kb:en-us:329405>. MS

changed some security stuff after which users who are not admins cannot resolve names. The fix worked for us.

Thank you, Tony.

Tony Gordon, Windows 2000 MCSE

tony.gordon@hewitt.com

Windows Server Infrastructure

Phone: 847.295.5000 x14534

Fax: 847.295.8877

Hewitt Associates

"Turner, Keith (Contractor)" <Keith.Turner@tea.army.mil>

01/31/2003 12:33 PM

To: focus-ms@securityfocus.com

cc:

SecurityFocus Microsoft: RE: Secure Ldap call not working due to IUSR/IWAM permissions?

Subject: Secure Ldap call not working due to IUSR/IWAM permissions?

I am trying to get LDAP working so that I can authenticate web users against an iPlanet directory server. There appears to be something on the machine which prevents IUSR or IWAM from making the LDAP call. My best guess is that something which was done during server "hardening" is preventing this from working. When using network monitor, I see that no packets are placed on the network. I have enabled auditing for global system objects and it does show audit failures when the LDAP call fails. I have used FileMon and RegMon (sysinternals) to watch for file or registry failures, but none showed up.

There about 20 fails for each LDAP attempt, but there are only two unique events

1) id 595
Indirect access to an object has been obtained
object type: port
object name: \RPC Control\DNSResolver
Accesses: Communicate using port

2) id 560
Object name: \Device\NetBT_Tcpip_{alphanumeric string}
Accesses: Synchronize, ReadData, WriteData

If I replace the hostname in the opensubject call with the ip address, the call makes it to the server (can see it in network monitor), but then fails.

I assume it is failing because the ip address doesn't match the hostname provided in the SSL certificate. If I place the IUSR/IWAM accounts in the local admin group, everything works properly (calling the directory server by hostname). The error always occurs on this line of the asp file :
Set oContainer = oLDAP.OpenDSObject(Server & dnUserName, dnUserName, sPassword, 2)

Anyone have any ideas?
Thanks, Keith

RE: Secure Ldap call not working due to IUSR/IWAM permissions?