

[NT] Flaw in SMB Signing Could Enable Group Policy to be Modified

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-12/0039.html>

From: support@securiteam.com

Date: 12/12/02

From: support@securiteam.com

To: list@securiteam.com

Date: 12 Dec 2002 17:44:42 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

Flaw in SMB Signing Could Enable Group Policy to be Modified

SUMMARY

Server Message Block (SMB) is a protocol natively supported by all versions of Windows. Although nominally a file-sharing protocol, it is used for other purposes as well, the most important of which is disseminating group policy information from domain controllers to newly logged on systems. Beginning with Windows 2000, it is possible to improve the integrity of SMB sessions by digitally signing all packets in a session. Windows 2000 and Windows XP can be configured to always sign, never sign, or sign only if the other party requires it.

A flaw in the implementation of SMB Signing in Windows 2000 and Windows XP could enable an attacker to silently downgrade the SMB Signing settings on an affected system. To do this, the attacker would need access to the session negotiation data as it was exchanged between a client and server, and would need to modify the data in a way that exploits the flaw. This would cause either or both systems to send unsigned data regardless of the signing policy the administrator had set. After having downgraded the signing setting, the attacker could continue to monitor the session and change data within it; the lack of signing would prevent the communicants from detecting the changes.

Securiteam: [NT] Flaw in SMB Signing Could Enable Group Policy to be Modified

Although this vulnerability could be exploited to expose any SMB session to tampering, the most serious case would involve changing group policy information as it was being disseminated from a Windows 2000 domain controller to a newly logged-on network client. By doing this, the attacker could take actions such as adding users to the local Administrators group or installing and running code of his or her choice on the system.

DETAILS

Affected Software:

- * Microsoft Windows 2000
- * Microsoft Windows XP

Mitigating factors:

- * A fix for this issue is already included in Windows XP Service Pack 1.
- * Exploiting the vulnerability would require the attacker to have significant network access already. In most cases, the attacker would need to be located on the same network segment as one of the two participants in the SMB session.
- * The attacker would need to exploit the vulnerability separately for each SMB session he or she wanted to interfere with.
- * The vulnerability would not enable the attacker to change group policy on the domain controller, only to change it as it flowed to the client.
- * SMB Signing is disabled by default on Windows 2000 and Windows XP because of the performance penalty it exacts. On networks where SMB Signing has not been enabled, the vulnerability would pose no additional risk – because SMB data would already be vulnerable to modification.

Patch availability:

Download locations for this patch

Microsoft Windows 2000:

- * All languages except NEC Japanese –

<http://microsoft.com/downloads/details.aspx?FamilyId=52EAC216-A360-4E2D-9C6B-AD4D31C40BA2&displaylang=en>

- * Japanese NEC –

<http://microsoft.com/downloads/details.aspx?FamilyId=F4119765-846B-491C-B162-BE06BD432828&displaylang=ja>

Microsoft Windows XP:

- * 32-bit Edition –

<http://microsoft.com/downloads/details.aspx?FamilyId=77B49431-742B-4426-AD45-F09D3AED16CB&displaylang=en>

- * 64-bit Edition –

<http://microsoft.com/downloads/details.aspx?FamilyId=580FCE68-B7E2-4BF9-8A16-54D1E39F2168&displaylang=en>

What's the scope of the vulnerability?

This vulnerability could provide a means by which a communications channel that is ostensibly cryptographically protected could in reality be unprotected. In the most serious case, exploiting the vulnerability could

Securiteam: [NT] Flaw in SMB Signing Could Enable Group Policy to be Modified

enable an attacker to change security policy information as it flowed from a Windows 2000 domain controller to a newly logged on system, thereby gaining the ability to take actions such as installing and running programs on the system.

Exploiting the vulnerability would require the attacker to not only have access to the network's communications media, but to also have a favorable location within the network. In addition, the attacker would need to exploit the vulnerability separately for every communications session he or she wanted to modify.

What causes the vulnerability?

The vulnerability results because of an error in the Windows 2000 and Windows XP implementations of the SMB signing function that could cause signing to not be done even when it's configured to always be required.

What is SMB?

SMB (Server Message Block) is a file-sharing protocol that is natively supported in all versions of Windows. SMB (and its follow-on, Common Internet File System) allows users and computers to efficiently locate and access files on other systems, and work with the data in them without creating conflicts with other users.

What is SMB signing?

SMB signing is a feature available in Windows 2000 and Windows XP, through which all communications using the Server Message Block (SMB) protocol can be digitally signed at the packet level. Digitally signing the packets enables the recipient of the packets to confirm their point of origination and their authenticity – that is that they came from the expected location and haven't been tampered with in transit.

Why would someone want to digitally sign SMB traffic?

The most straightforward reason is that a user might want to ensure that any files he or she retrieves from, for instance, a file server haven't been altered in transit by an attacker on the network. But there's a more pressing reason. Windows domains use SMB to transfer some types of security related information. For instance, when a workstation logs onto a domain, the domain controller sends group policy information to the workstation via SMB. Signing provides a way to ensure that the workstation is receiving bona fide group policy.

How is SMB Signing configured?

SMB Signing is configured via local policy settings (specifically, Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options). There are four settings available: two govern how the system operates when acting as a client, and two govern how it operates when acting as a server. In each case, the system can be configured to allow, disallow, or require signing. The system defaults for both Windows 2000 and Windows XP enable signing but do not require it.

Securiteam: [NT] Flaw in SMB Signing Could Enable Group Policy to be Modified

What's wrong with the way SMB Signing is implemented?

There's a flaw in the way Windows 2000 and Windows XP respond in the case where a system has been configured to require signing. By design, when a Windows 2000 or Windows XP system establishes an SMB session with another system, it carries out a negotiation to determine what the other system's signing requirements are. If the other system can't or won't meet its needs (for instance, if a Windows XP system were configured to require signing but the other system was configured never to sign SMB data), it should refuse to establish the communications channel.

A security vulnerability results because, if the negotiation information were malformed in a particular way, a Windows 2000 or Windows XP system that had been configured to require signing could instead silently drop the requirement, and engage in unsigned communications despite the local policy settings.

What could an attacker do via this vulnerability?

An attacker could use this vulnerability to cause SMB signing on a Windows 2000 or Windows XP system to be silently disabled for the duration of an SMB session, with the result that the subsequently transmitted data would be unsigned. This would enable anyone who could access the data to modify it as it transited the network.

All SMB sessions, whether used to transfer files, group policy, or some other information, could be affected by the vulnerability. However, it would pose the greatest risk in the case of group policy – specifically, where a Windows 2000 domain controller had been configured to require SMB signing, as a way of ensuring the authenticity of the group policy settings it downloads to domain members. By exploiting the vulnerability and then subsequently changing the group policy data as it was sent from the domain controller to a client, the attacker could change the policy settings that the client received.

What would be the effect of changing the group policy settings?

It would depend on the specific changes. However, group policy is a powerful technology through which much of the behavior of Windows systems can be controlled. For instance, group policy can be used to change permissions on folders and files, download and run programs at system startup, and take other actions.

Would the attacker be able to use the vulnerability to gain administrative privileges on the domain?

No. Domain group memberships are held at the domain controller, not the client. Changing the group policy that's downloaded to the client wouldn't allow the attacker to change his or her domain group memberships. On the other hand, the attacker could use the vulnerability to change the group memberships on the local machine and, for instance, add users to the local Administrators group.

Who could exploit the vulnerability?

In order to exploit the vulnerability, the attacker would need to already

Securiteam: [NT] Flaw in SMB Signing Could Enable Group Policy to be Modified

have a significant degree of access to communications on the network. He or she would need to be able to monitor and modify the communications between the two systems in real-time. This would typically require the attacker to not only have physical access to the network media, but a favorable location within the network as well.

What do you mean "a favorable location within the network"?

It wouldn't be enough for the attacker to have access to the network media. He or she would also have to be located along the path taken by the data as it passed between the client and the server. The vulnerability provides no way for the attacker to force the communications to take a particular path so, in most cases, he or she would need to be located on the same network segment as one of the two communicants.

Could the attacker change group policy on a system that was already logged onto the domain?

No. The opportunity to impose new policy would occur when a new system logged onto the domain. If the attacker missed the opportunity, he or she would need to wait until the next time the system logged on.

Would exploiting the vulnerability once permanently disable SMB signing?

No. The attacker would need to exploit the vulnerability separately for each communications session that he or she wanted to interfere in.

Could the attacker change the group policy on the Windows 2000 domain controller?

No. The vulnerability would only allow the attacker to change the data received by the client. It would not provide any way to change the data as it resides on the server.

Why have you discussed the domain controller scenario only in the context of Windows 2000?

Windows XP cannot be used as a domain controller. As a result, this scenario – which is the highest-risk scenario associated with the vulnerability – doesn't apply to Windows XP.

I heard that Windows XP clients can inadvertently trigger the vulnerability. Is this true?

Yes. Windows XP Service Pack 1 contained a regression error that adds information to the negotiation information it sends. This information can trigger the vulnerability, and cause systems running Windows XP Gold or Windows 2000 to drop SMB signing. A fix is available to eliminate this regression error.

It is important to understand two critical points regarding the regression error in Windows XP Service Pack 1:

* The regression error poses no security threat to Windows XP Service Pack 1 systems. Instead, it poses an availability risk. Consider a scenario where both a Windows XP SP1 system and a Windows 2000 domain controller were configured to require signing. The regression could cause the Windows 2000 system to downgrade its signing, which the Windows XP SP1

Securiteam: [NT] Flaw in SMB Signing Could Enable Group Policy to be Modified

system would then reject. The result would be that the communications couldn't occur.

* Installing the fix for the regression error in Windows XP doesn't eliminate the vulnerability. The vulnerability lies in Windows XP Gold and Windows 2000; the regression error simply triggers it in some cases. If you apply the security patch to all Windows XP Gold and Windows 2000 systems that require signing, it doesn't matter whether you apply the regression fix to your Windows XP SP1 systems – if no systems on the network have the vulnerability, it doesn't matter whether there are systems that could inadvertently trigger it.

I don't understand. You said in the preceding question that Windows XP Service Pack 1 has a regression error associated with the vulnerability, but in the "Additional Information About This Patch" section you say that it doesn't need the patch. Why is this?

Windows XP Service Pack 1 does not have the vulnerability. That is, no matter what negotiation information is sent to it, Windows XP Service Pack 1 will not silently drop SMB Signing. However, it does have an error that can cause it to send negotiation information that exploits the vulnerability in other systems.

Should I apply the patch to every Windows 2000 or Windows XP system? You can, but it only makes sense to install it on systems that are configured to require SMB Signing, or that communicate with systems that do.

Is SMB signing required by default?

No. There is a performance penalty associated with SMB signing, and as a result it is not required in default configurations of Windows 2000 or Windows XP.

SMB signing isn't enabled on my systems. Am I at any risk from this vulnerability?

If SMB signing isn't enabled, your network is at no increased risk because of this vulnerability. That is, if signing is disabled, an attacker could already modify the SMB data stream.

How does the patch address the vulnerability?

The patch causes Windows 2000 and Windows XP to correctly handle negotiation sessions that contain the type of malformed information discussed above.

ADDITIONAL INFORMATION

The information has been provided by

<mailto:0_42043_E51E4D7D-DECD-43AE-9A29-36080E8D4C3C_US@Newsletters.Microsoft.com>
Microsoft Product Security.

=====

Securiteam: [NT] Flaw in SMB Signing Could Enable Group Policy to be Modified

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.