

Re: QFE Installer Error

Source: <http://www.tech-archive.net/Archive/Windows/microsoft.public.windowsupdate/2004-03/0522.html>

From: Torgeir Bakken (MVP) (Torgeir.Bakken-spam_at_hydro.com)

Date: 03/03/04

Date: Thu, 04 Mar 2004 00:27:32 +0100

Rod wrote:

> I followed the step you said to the letter, but I still receive the QFE Installer Error. Here are the last 20 lines of my Windows Update.log as you requested.

> [snip]

> Here is some additional info that might help. This is the link where I downloaded the file Q329170.

>

<http://www.microsoft.com/downloads/details.aspx?FamilyID=803a07d2-221f-46d6-9679-76170ab435ab&display=details>

> This is the full name of the file. Q329170_XPE_SP2_X86_ENU.exe

Hi

This update has a severity rating of "Low" for Windows XP, I would just have skipped the update.

As I see it, you take no big risk by not installing it:

>From the "Technical details" section at

<http://www.microsoft.com/technet/security/bulletin/MS02-070.asp>

("Flaw in SMB Signing Could Enable Group Policy to be Modified (329170)")

<quote>

Mitigating factors:

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

microsoft.public.windowsupdate: Re: QFE Installer Error

SMB Signing has not been enabled, the vulnerability would pose no additional risk – because SMB data would already be vulnerable to modification.

Severity Rating:

Windows 2000: Moderate

Windows XP: Low

The above assessment is based on the types of systems affected by the vulnerability, their typical deployment patterns, and the effect that exploiting the vulnerability would have on them. The threat to Windows XP systems is lower than for Windows 2000 systems because the most serious potential outcome of exploiting the vulnerability – modifying group policy as it is disseminated by a domain controller – does not apply to Windows XP, since it cannot serve in such a function.

</quote>

and from the FAQ section:

<quote>

Who could exploit the vulnerability?

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

</quote>

--

torgeir

Microsoft MVP Scripting and WMI, Porsgrunn Norway

Administration scripting examples and an ONLINE version of the 1328 page

Scripting Guide: <http://www.microsoft.com/technet/community/scriptcenter/default.mspx>