Things to know about Windows HCP errors

If you are using Windows XP or Windows Server 2003, you must upgrade your registry - or someone can run software or commands on your computer as if they were friends.

Network administration - If you are using Windows XP or Windows Server 2003, you must upgrade your registry - or someone can run software or commands on your computer as if they were friends.

Anyone using Windows XP or Windows Server 2003 needs to upgrade the registry to temporarily fix this error.

A serious error in the Help and Support center has just been published recently and Microsoft has not had an official patch yet and no assessment of when it will fix this problem. Worse, a simple code that can exploit this error can be found quite easily, along with detailed explanations, making it easy to use by bad guys who want to exploit it. Exploiting vulnerabilities in the operating system.

The problem must somehow be able to handle HCP: // links. Common website links use HTTP and the HCP links used by Help and Support Center (helpctr.exe).

Users may think that being infected is caused by clicking on a link, in a web page or an email. But the truth is not that, watching a website seems harmless but it all comes from there. Microsoft Security Advisory (2219475) has warned that 'This vulnerability could allow remote code execution if a user views a fake website using a web browser .'

If this error is exploited, bad guys can run software or commands on your computer, as if they were friends. The last phrase is very important but not emphasized in the articles that I have read about this topic.

Anyone who logs on to Windows as an administrator must be affected by the vulnerability like those who don't know anything. Operating as a restricted user ("limited" is a term commonly used by Windows XP) does not protect you from HCP errors, however it limits what the software is malicious or anyway. The commands can be executed on your computer.

Simply, bad guys will not be able to exploit this error to install the software when you log in as a restricted user. They can run malicious software, but the software cannot be permanently installed and there are some restrictions on what it can do. Obviously, that's the whole idea behind the restricted users.

But rarely does anyone run as a restricted user.

Big mistake.

The patch is currently provided

Needless to say, the best way to prevent what malicious code can attack is to perform a registry upgrade. Until Microsoft fixes the problem at a fundamental level, the temporary patch that Microsoft suggests involves Windows not processing any HCP links.

First, upgrading the registry to bypass the HCP links needs to be done manually, but Microsoft has provided a tool that can automatically perform that task for you.

Regardless of how the registry will be upgraded, before you do anything with the registry you need to create a backup for it first. With Windows XP, click Start -> Programs -> Accessories -> System Tools -> System Restore. Click the "Create a restore point" option and name it something like "before disabling the HCP protocol".

We see there are two different suggested methods for performing manual registry upgrades - one is to delete the data in the registry, the other is to change the name to reduce the havoc.

The way we like it and use it here is to change the name. Steve Gibson provided enough information about this method on the HCP 0-Day Quick Fix blog.

In a nutshell, run regedit, perform a search with the keyword "HCP" (value or data) and match the whole string. After finding it, rename it, that's all. Note that the Find command does not distinguish between letters or lowercase letters. You need to log in as an administrator to change the registry.

If you don't like to deal with the registry directly, you can use Microsoft 'Fix it' patch here.

This method will force you to download a file, MicrosoftFixit50459.msi to your computer and run it. One advantage of this method is that you can download the file once and use it to fix many computers.

There are not many problems but the Microsoft Fix it does not rename the HCP registry key, nor does it delete the component, but instead deletes the subkeys below the HCP in the registry.

You will see the 'Microsoft Fix Internet' page with links that allow and disable temporary patch (workaround). Don't be confused - "enable" (also known as Microsoft Fix it 50459) refers to disabling the HCP protocol. The "disable" option (known as Microsoft Fix it 50460) is needed in the future after Microsoft fixes the underlying problem.

Again, many XP users should not use Help and Support center. If that is you, you can leave the HCP protocol disabled forever. It has been abused before.

Ki?m TRA

The person who discovered this error provided two typical mining cases. You can verify that disabling the HCP protocol can prevent the problem by running these tests first.

Windows XP users using Internet Explorer 7 can click on the link below to test the vulnerability.

http://lock.cmpxchg8b.com/b10a58b75029f79b5f93f4add3ddf992/starthelp.html

If the calculator calculator of Windows starts, your computer will have a vulnerability.

Windows XP users who are using Internet Explorer 8 and Windows Media Player 9 can click the link below to test the vulnerability.

http://lock.cmpxchg8b.com/b10a58b75029f79b5f93f4add3ddf992/launchurl.html

Next, if Windows' calculator is launched, your computer will also have vulnerabilities. If you have installed a new version of Media Player, this is not a valid test.

According to the developer:

There must be some changes to other configurations, which is simply an attempt to prove the problem . In addition, our proof is not intended for the purpose of stealing, a real attack. will rarely warn victims . Browsers are also very useful for demonstrating problems, but there are certainly many other attack methods, such as BUY, documents, . Administrators Protocol logic designed to be used between applications.

It should be noted that, when the antivirus / anti-malware software on the computer can detect these examples as malicious code, that doesn't mean that it has complete protection for the problem.

To ensure that the registry upgrade disables the HCP protocol that is actually doing its job, you can disable your antivirus software, run the test to see if the Calculator is called, run the patch, Then run the test again to make sure the Calculator is not running.

Disable the underlying service

Finally, there is no other way to solve this problem, before Microsoft released the patch - disabling the Help and Support service below is the solution to do now.

We did this on one of our computers while running one of the tests, before disabling HCP. On that computer, we disabled the service before since it rarely used Help and Support Center. IE7 has warned that the service needs to be started and the Calculator is not running.

This solution is not recommended by Microsoft, but it will create a good second defense.

Interesting, when disabling the service again prevents exploitation of the test, while merely stopping the service is not. This is because, with the service configured manually, the exploit test can launch the service and run the Calculator. However, disabling the Help and Support service may not be a solid defense, we found the service launcher software has been disabled.

For greater certainty, if the HCP protocol is disabled, the computer will be protected even if the Help and Support service is running.

When upgrading the registry, adjusting the status of the service requires administrator level authentication.

Any user running Windows 7, Vista, 2000 or Server 2008 is not affected. The problem with the HCP protocol only affects Windows XP and Server 2003 users.

Microsoft's semi-automatic 'Fix it' solution will create a restore point called "Installed Microsoft Fix it 50459". However, the Fix it program will upgrade the registry despite problems with System Restore, so we feel it is the best solution for creating manual restore points so that you can verify that all are real. good upgrade of the registry.