

How to fix BlueKeep security error for Windows 2003, Windows XP, Windows 7, Windows Server 2008

To fix the BlueKeep security vulnerability, users need to disable RDP and block port 3389

The new BlueKeep security vulnerability that attacked older versions of Windows in May affected about a million devices. BlueKeep not only attacks Windows 7 but also affects Windows 2003, Windows XP, Windows Server 2008 and Windows Server 2008 R2. Soon Microsoft released a patch for all Windows versions affected by BlueKeep. But one has not yet updated the patch and is in danger of being attacked by the BlueKeep vulnerability. The following article will show you how to fix security holes on old Windows versions.

1. What to do if Google Chrome warns an unsafe website?
2. 10 most effective antivirus software for Windows
3. 9 things to do when detecting a computer infected with malware
4. 3 things that antivirus software can't do

Instructions to fix BlueKeep error on Windows

Security vulnerability BlueKeep uses remote computer control protocol - Remote Desktop Protocol (RDP) of Windows to remotely access users' computers. This vulnerability allows pre-authentication and does not require user interaction for hackers to execute code on the computer system. Once they have access to the computer, they will view, change, delete all data.

First of all, users need to check if their computer is vulnerable to this security vulnerability. We download rdpscan tool according to the link below.

<https://github.com/robertdavidgraham/rdpscan/releases>

Step 1:

We download the patches in the 2 links below and then proceed with the installation. Windows Update mode on the computer fades to turn on.

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708>

<https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708>

Platform	Article	Download	Impact	Severity
Windows XP SP3 x86	4500331	Security Update	Remote Code Execution	Critical
Windows XP Professional x64 Edition SP2	4500331	Security Update	Remote Code Execution	Critical
Windows XP Embedded SP3 x86	4500331	Security Update	Remote Code Execution	Critical
Windows Server 2003 SP2 x86	4500331	Security Update	Remote Code Execution	Critical
Windows Server 2003 x64 Edition SP2	4500331	Security Update	Remote Code Execution	Critical
Windows Server 2003 R2 SP2	4500331	Security Update	Remote Code Execution	Critical
Windows Server 2003 R2 x64 Edition SP2	4500331	Security Update	Remote Code Execution	Critical
Windows Vista SP2	4499180	Security Update	Remote Code Execution	Critical
Windows Vista x64 Edition SP2	4499180	Security Update	Remote Code Execution	Critical

Step 2:

Next we proceed to disable RDP and block port 3389. To disable RDP you open CMD on the Admin computer, then enter the command below.

```
Reg add 'computernameHKLM SYSTEMCurentControlSetControlTerminal Server' /v fDeny'
```

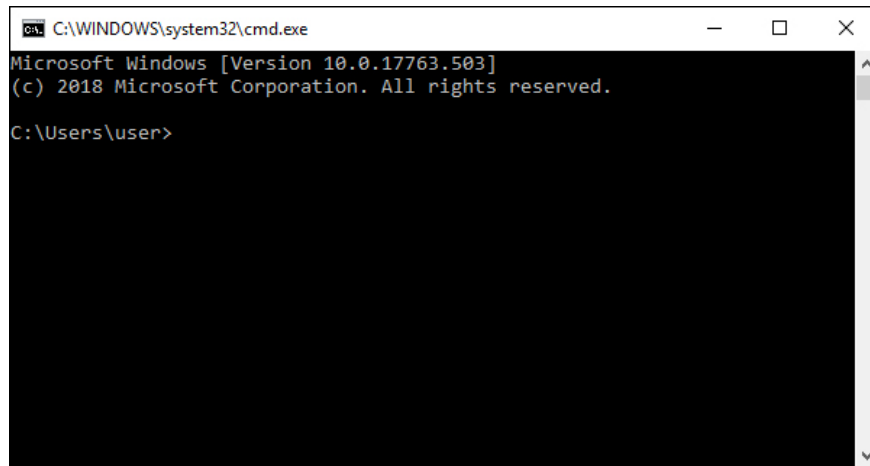
```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.503]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\user>

```

Click the following command to block port 3389

```
netsh advfirewall firewall add rule dir=in action=block protocol=TCP localport=3
```



I wish you all success!

You finished reading the article "**How to fix BlueKeep security error for Windows 2003, Windows XP, Windows 7, Windows Server 2008**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.