NHS Digital

Guide to patching

Published 14 May 2017

Information and technology
for better health and care

How and when this guide should be used and what help is available

NHS Digital delivers a range of data security services that support health and care organisations to take appropriate cyber security measures and help them to respond effectively and safely to cyber security threats. These include:

- broadcasting information to NHS organisations about known cyber security threats and appropriate steps to take to minimise these risks, as was the case with this incident.
- protective real-time monitoring of national NHS IT services and systems, which have all been designed to have strong security measures.
- Undertaking free cyber security testing for NHS organisations and give them bespoke advice about appropriate steps they can take.
- training for health and care staff designed to ensure frontline workers are aware of their own responsibility towards ensuring cyber security in their organisations, and that they know the simple steps that they can take to help to keep their organisation secure.

To receive NHS Digital's high-severity security threat alerts and advisories on data security please email carecert@nhsdigital.nhs.uk

In respect to using this guide you should only apply patches to your local machines/computer if you are sure that:

- the machines/computers you intend to patch have not already been patched either virtually or by someone else, **if you're unsure please contact your local IT provider, this could be your CSU or similar.**
- you are confident after reading the guide that you believe you can implement the patch.

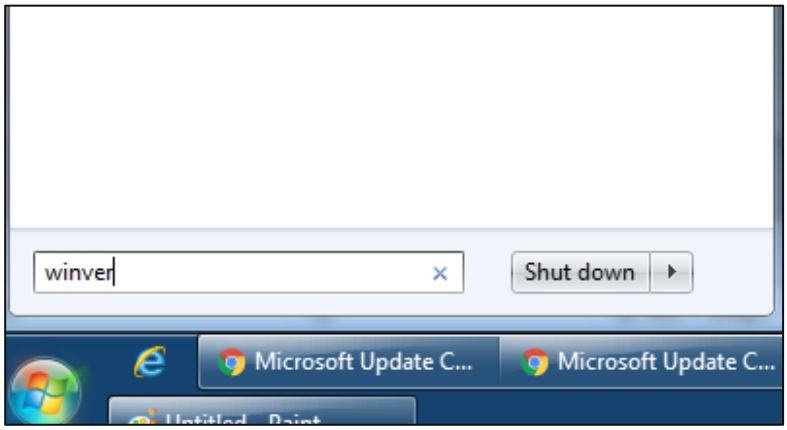
If you are content to proceed this guide will enable you to:

- Identify the right version of Windows and the service pack to ensure you can successfully patch your computer
- Show you how to identify and download the patch
- Give you the basic steps to start the implementation.

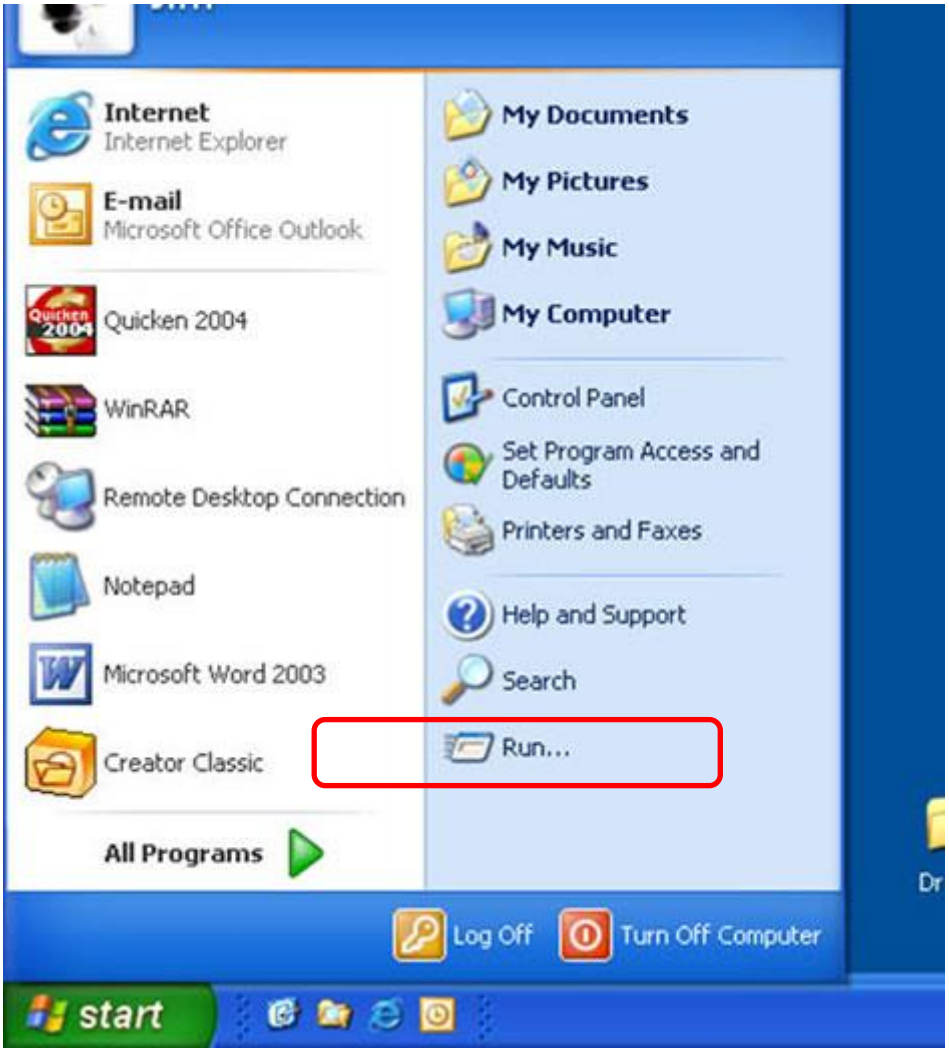
If you do not know what operating system you use:

- If you don't know which operating system you are running, you can go to the Start menu and type "winver" in the search box, or click the 'Run' icon, and type "winver" in the box that appears:

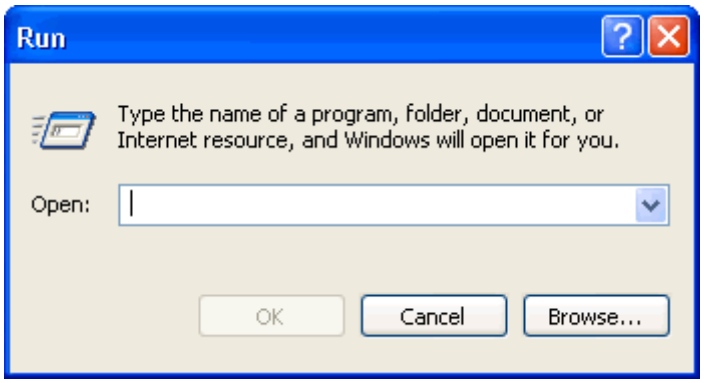
The search box on the start menu looks like this:



If you use the 'run' icon this is where you find it on the start menu:



The ‘run’ icon will look like this, remember to type winver and press ‘OK’ to see your windows version:

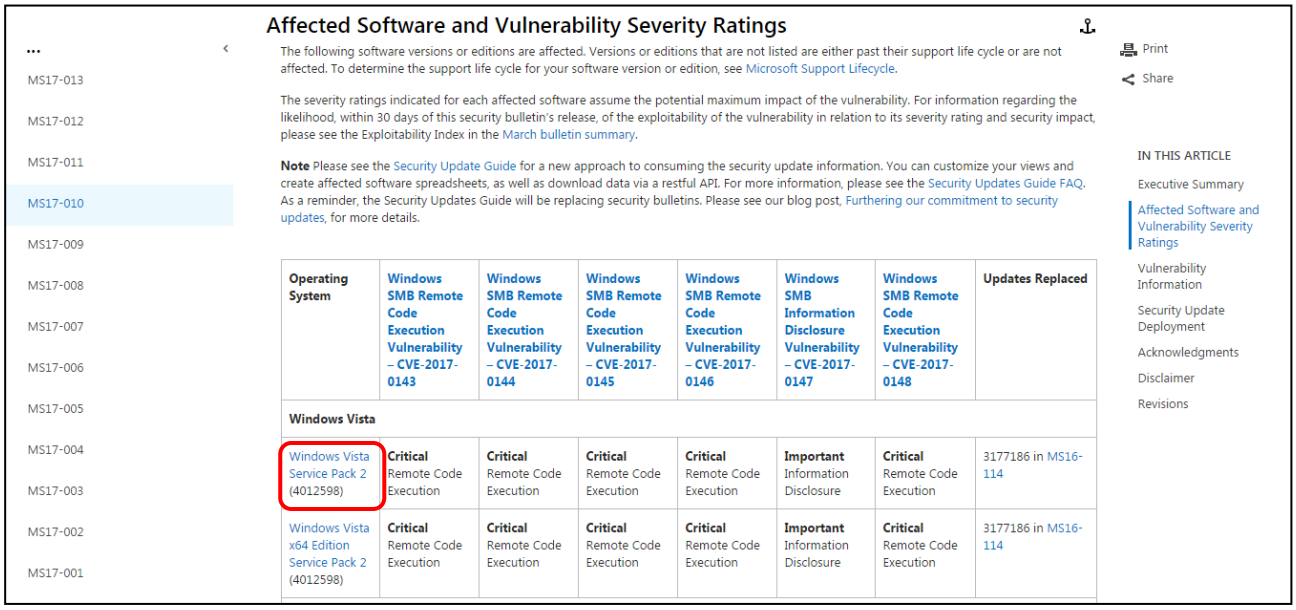


About Windows” will tell you the version and Service Pack you are running, a pop up box as below will have the information. As you can see here it states the windows version in Windows 7.

The next thing you need to do once you know you’re Window version, is to find the right patch for your Windows version. This means going to a safe and secure Microsoft website to download the patch. So this is what you need to do:

- Click the link below, or if this is not possible copy and paste it into your web browser (as a last resort type it in) and then search the list of operating systems to find the patch that matches your Windows version. SO here is the link you need to go to: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

- The screen shot below is what the website will look like:



Affected Software and Vulnerability Severity Ratings

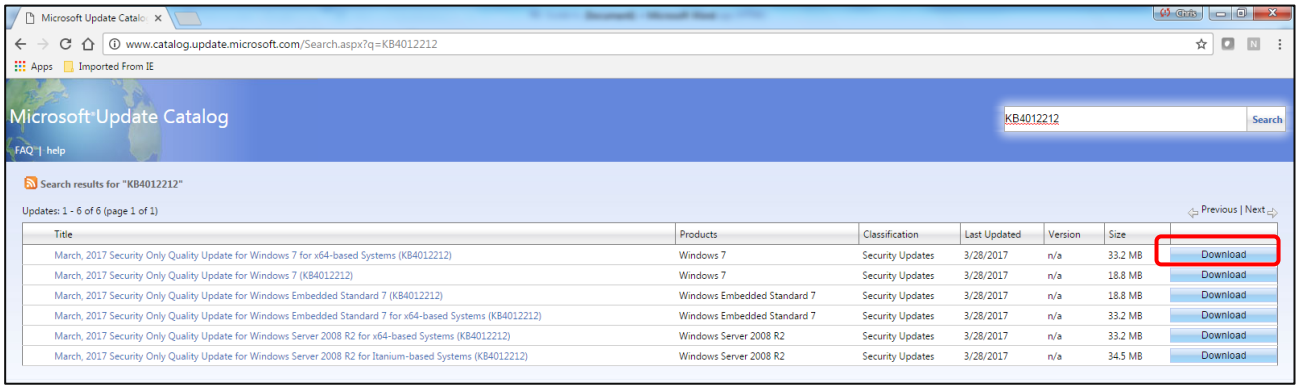
The following software versions or editions are affected. Versions or editions that are not listed are either past their support life cycle or are not affected. To determine the support life cycle for your software version or edition, see Microsoft Support Lifecycle.

The severity ratings indicated for each affected software assume the potential maximum impact of the vulnerability. For information regarding the likelihood, within 30 days of this security bulletin's release, of the exploitability of the vulnerability in relation to its severity rating and security impact, please see the Exploitability Index in the March bulletin summary.

Note Please see the Security Update Guide for a new approach to consuming the security update information. You can customize your views and create affected software spreadsheets, as well as download data via a restful API. For more information, please see the Security Updates Guide FAQ. As a reminder, the Security Updates Guide will be replacing security bulletins. Please see our blog post, Furthering our commitment to security updates, for more details.

Operating System	Windows SMB Remote Code Execution Vulnerability – CVE-2017-0143	Windows SMB Remote Code Execution Vulnerability – CVE-2017-0144	Windows SMB Remote Code Execution Vulnerability – CVE-2017-0145	Windows SMB Remote Code Execution Vulnerability – CVE-2017-0146	Windows SMB Information Disclosure Vulnerability – CVE-2017-0147	Windows SMB Remote Code Execution Vulnerability – CVE-2017-0148	Updates Replaced
Windows Vista							
Windows Vista Service Pack 2 (4012598)	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3177186 in MS16-114
Windows Vista x64 Edition Service Pack 2 (4012598)	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Critical** Remote Code Execution	**Important** Information Disclosure	**Critical** Remote Code Execution	3177186 in MS16-114

- Click the link on the relevant operating system to open the Microsoft Update Catalog (we've put a screen here below this bullet) then download the relevant update for your Windows version:

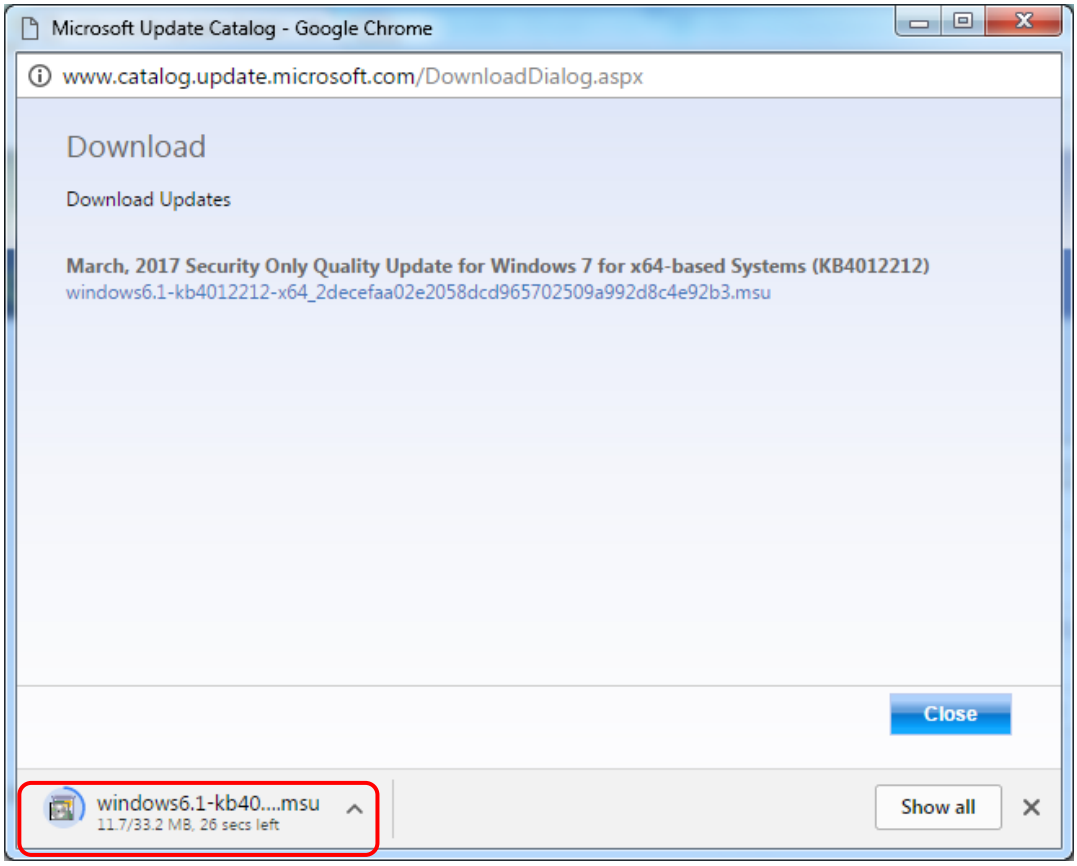


Microsoft Update Catalog

Search results for "KB4012212"

Title	Products	Classification	Last Updated	Version	Size	
March, 2017 Security Only Quality Update for Windows 7 for x64-based Systems (KB4012212)	Windows 7	Security Updates	3/28/2017	n/a	33.2 MB	Download
March, 2017 Security Only Quality Update for Windows 7 (KB4012212)	Windows 7	Security Updates	3/28/2017	n/a	18.8 MB	Download
March, 2017 Security Only Quality Update for Windows Embedded Standard 7 (KB4012212)	Windows Embedded Standard 7	Security Updates	3/28/2017	n/a	18.8 MB	Download
March, 2017 Security Only Quality Update for Windows Embedded Standard 7 for x64-based Systems (KB4012212)	Windows Embedded Standard 7	Security Updates	3/28/2017	n/a	33.2 MB	Download
March, 2017 Security Only Quality Update for Windows Server 2008 R2 for x64-based Systems (KB4012212)	Windows Server 2008 R2	Security Updates	3/28/2017	n/a	33.2 MB	Download
March, 2017 Security Only Quality Update for Windows Server 2008 R2 for Itanium-based Systems (KB4012212)	Windows Server 2008 R2	Security Updates	3/28/2017	n/a	34.5 MB	Download

- Click the link within the pop up window to download the patch –as you can see below, the file will be seen at the bottom, in some versions the file may pop up or ask you to whether you would like to open. However, it will likely look like this:



- Click the downloaded file to run and follow instructions to install the patch; the instructions will be displayed on screen and all you need to do is follow the instructions, these should be self-explanatory.

- The machine should install the update and will need to restart, it will either restart automatically or ask you to restart, please restart the machine if you are asked to do so. Once the machine has restarted, the patch will be installed and this will give protection against the known cyber-attack.