

USING THE MICROSOFT BASELINE SECURITY ANALYZER

Beginners' Kaffee Klatch
Presented by Bill Wilkinson
August 21, 2010

You probably know that when Microsoft finds a security hole in Windows or Internet Explorer they release a patch called a "Critical Update" through their Windows Update service.

What you may not know is that Windows Update isn't always accurate. Windows Update frequently thinks you've installed a Critical Update that you haven't, leaving your computer vulnerable.

Fortunately, **Microsoft's Baseline Security Analyzer** [MBSA] takes care of that little-known problem. MBSA is a free program from Microsoft that scans for over 60 common system misconfigurations plus almost any Microsoft security update your computer may be missing. In particular, MBSA double-checks the security of:

- Windows (XP, Vista, and Win7)
- Microsoft Office 2000 and later
- Internet Explorer 5.01 and later
- Windows Media Player 6.4 and later
- A bunch of other Microsoft applications and services

MBSA analyzes, but you must fix! In other words, MBSA tells you what's wrong and points you to the solution. But YOU have to manually download and apply the solution. That's important to remember.

While the MBSA was designed for corporate tech support, there is no reason why you can't use it at home. It's **free**.

To get the latest version of Microsoft's MBSA, just go to <http://tinyurl.com/33k8ez8>

Download the MBSASetup-EN.msi file to your desktop.
Check the file for a possible virus. (we will show you how during the presentation.)

Double-click on the MBSASetup icon and follow the Installation Wizard commands.

Running MBSA

1. Once you've downloaded and installed MBSASetup-EN.msi, double-click on the MBSA "watering can" [padlock and checkmark] icon. This opens the MBSA welcome screen.
2. Click "Scan a computer."
3. On the next screen, don't change anything. Just make sure you are connected to the Internet and then click "Start scan."
4. MBSA calls home to Microsoft and downloads something called "MSSecure.cab." This file contains information about practically every patch Microsoft has released. MBSA scans your computer's operating system, system components, and Microsoft applications. MBSA then compares the version numbers of the Microsoft programs on your computer with the latest version numbers in the MSecure.cab file.
5. Finally, MBSA shows you which updates your computer is missing.

Interpreting the security report

Critical failures [red Xs] require you to immediately install a patch or update to ensure the strongest security for your computer. Non-critical failures [yellow Xs] happen when there is a newer version of something available, but you don't really have to upgrade yet. Best practices [blue asterisks] could signify a problem--MBSA can't confirm that those particular security updates have been installed.

What's important and what isn't? MBSA's security report has seven sections, but only two are important to home users.

1. Security Update Scan Results [at the top of the report]
2. Desktop Application Scan Results [at the very bottom]

Fixing the critical failures

Remember, MBSA analyzes, you fix.

To find a fix for a critical failure in the two sections mentioned above, click on the "Result Details" link next to that critical failure. This shows you exactly what's missing or is misconfigured. Click on each link and it opens a page in Internet

Explorer telling you how to download the appropriate patch. **REMEMBER TO INSTALL THE PATCHES AFTER YOU DOWNLOAD THEM!** MBSA won't do it for you.

Blue Asterisks

Sometimes MBSA gets confused and can't confirm if your computer has a particular patch. That's what the blue asterisks signify. Fixing those blue asterisks is a little more complicated.

1. Click on Results Details.
2. In the description for each Security Update you'll see a six digit number in parentheses. Write down each six digit set of numbers you see.
3. Then go to Add/Remove Programs in your Control Panel.
4. Scroll down towards the bottom and look for the Windows Hotfixes.
5. Compare those six digits you wrote down in MBSA with the last six digits of the various hotfixes in Add/Remove Programs.
6. If you find a match, you have the patch. MBSA just got confused. If you don't find a match, go back to the MBSA Results Details page and manually download and install the missing patches.

MBSA tips

Run MBSA from time to time (every three months or so) just to double-check your computer's security. Don't be surprised if MBSA still gives you blue asterisks even after you've installed all the patches. Sometimes MBSA gets confused and there's no real way to "unconfuse it."