TECHNICAL SERVICE BULLETIN (TSB)

Microsoft Update

KB2661254 — LOGGING INTO THE COMSIFTER

ComSifter®
protect web users now!

TSB Date: October 11, 2012

IN THIS DOCUMENT

- Scenario
- Problem
- Background
  Who is affected?
  Who is not affected?
- What to Do
- Resolution
- Summary

This TSB is to give guidance to the effects of Microsoft Update KB2661254.

SCENARIO

On Tuesday, October 10, 2012, Microsoft released update KB2661254. This update has resulted in a problem when logging into your ComSifter. Microsoft decided to force a large cryptographic key when using secure communications over the Internet. Any RSA key that is 1024-bits or less will no longer be supported. Microsoft did this without any method of excluding the millions of sites and equipment that use lower-sized keys.

PROBLEM

If you are using Internet Explorer, Safari or Opera and you log into your ComSifter you will be presented with a security warning. When you click on "Continue to this website" as you have done many times before, nothing happens. There is no warning or explanation.

Note: The above description of the problem is what happens with Internet Explorer. Other browsers may not even allow the security warning for the certificate to show.

Note: Mozilla Firefox does not appear to be affected by this update.

BACKGROUND

When you open a browser and go to a secure site (HTTPS), a negotiation between the computer you are using and the remote site is performed using the information that is contained in what is referred to as a certificate. The certificate includes information as to how the cryptographic keys are to be used. This information includes the size of the keys. As computing power has increased, so has the need to increase the size of these security keys.

Comsift uses a secure connection when you log into and configure the ComSifter, and has always used a 1024-bit key. This provides a good level of security during the period of time that you are configuring the ComSifter.

Microsoft has decided that they will force the use of keys larger than 1024-bits, and in the process have crippled many pieces of equipment and websites, including the following ComSifter appliances:

Who is affected?

Note: Only logging into the ComSifter is affected. Normal Internet traffic is not affected unless the user is going to a website that is affected by this update.

The following models are affected—only if KB2661254 has been installed:

CS-1B	CS-1C
CS-8B	
CS-8 Pro	CS8 Pro NS

Who is not affected?

Legacy CS-1 and Legacy CS-8

CONTINUED

Comsift, Inc. | **1646 Elderberry Way, San Jose, CA 95125-4507** | **866-875-1254** | **info@comsift.com** | **www.comsift.com**

All ‘D’ units
Users of Mozilla Firefox

RESOLUTION

- If you do not install the Microsoft Update KB2661254, you will not be affected.
- Use Mozilla Firefox to communicate with the ComSifter
- If the update is installed and you wish to use Internet Explorer, Safari or Opera you must uninstall it if you wish to configure your ComSifter.

The following instructions are for a Windows 7 operating system. Windows XP and Windows Vista are similar.

1. Log into your computer using an administrator rights account.
2. Open “Control Panel”
3. Open “Windows Update”
4. Open “View Update History”
5. At the top of the page click on “Installed Updates” in the sentence containing “To remove and update…”
6. Find and right-click “Update for Windows 7 for x64-based Systems (KB2661254)”
7. Click “Uninstall.”
8. Restart the computer.
9. Important: After restarting, go back into the update section (for new updates) and uncheck this update. To keep it from re-installing, right-click and select “Hide.”
   Note: Failure to hide the update will result in the update being re-installed later.

SUMMARY

Comsift believes Microsoft has not realized the full effect that his update will have on the installed base of the Internet. We believe that they may either roll back this update or at least provide a selective method of bypassing it.

Meanwhile, Comsift will be exploring potential software updates to some of our models to increase the key length.

Comsift, Inc. | 1646 Elderberry Way, San Jose, CA 95125-4507 | 866-875-1254 | info@comsift.com | www.comsift.com