

Stay Smart Online Alert Service Newsletter

September 2008

Overview

The purpose of the Newsletter is to provide general advice about online security issues and help you learn to better manage the security of your computer and information when online.

The Newsletter provides additional information about the threats and software bugs which were reported during the period, or about other threats to be aware of.

Feedback

Thank you to those subscribers who have provided feedback to our Alerts, Advisories and Newsletters. We are very interested in your feedback and where possible take on board your suggestions or requests. In this newsletter we have responded to a question asked by one person.

This is just a reminder that if you wish to modify your subscription preferences, you need to login and supply your password to authorise these changes. We have prepared a [Frequently Asked Question \(FAQ\)](#) which explains how to do this.

User software bugs

Since the last newsletter was published, the Stay Smart Online Alert Service has published alerts and advisory about a range of Microsoft and Apple products. These alerts and advisories have included bugs in both operating systems and application software for client and server computers. Server computers are generally used by businesses. Servers are computers which other computers connect to. For example a web pages or a web site is hosted on a web server. Client computers (used by people) connect to the web server in order to view the pages on the web site.

The operating system is the base software installed on a computer which controls all input and output hardware devices and drivers such as monitor, keyboard, mouse, printer etc, and system memory, processing and disk resources required by user software installed on the computer.

User software (also called application software) allows users to undertake specific tasks, such as play games, create documents, view videos files, browse the web, read email, create and edit spreadsheets etc.

Home users often neglect to fully update application software, generally because there is more of it and it takes more time to do so if automatic updates are not available or turned on. Also sometimes users forget or don't realise particular software is installed on their computer and needs to be updated.

For example, earlier this month, the Stay Smart Online Alert Service published an [alert](#) about security bugs in QuickTime, which need to be fixed. This is an example of user software that may be installed but is not always updated when new bugs are disclosed. Fortunately, this software can be set to update automatically.

QuickTime

QuickTime is a free media streaming (including audio and video) software produced by Apple but versions exist for both Microsoft Windows and Apple Mac operating systems. QuickTime is installed by default on Apple Mac OS X and may be bundled and installed with iTunes and the Safari web browser on Microsoft Windows.

QuickTime may be set to update automatically or manually. To check if your QuickTime update is set to automatically update, open QuickTime, go to the “Help” menu and select “Update Existing Software”. This will open a new window which includes the checkbox “Check for Updates Automatically”. To turn automatic updates on, make sure this box is ticked.

What you can do

Most operating systems and many application software programs can be configured to update automatically. Make sure automatic updates are turned on when available.

If automatic updates are not available, then check for updates manually on a regular basis – at least monthly.

Common online threats

Every day new malicious software is written and released by criminals over the Internet, either through spam email, or by installing malicious software on the world wide web (www).

It is important to know that the Stay Smart Online Alert Service is not able to provide a report on every single potential threat that users may encounter online – to attempt to do so may overwhelm most subscribers who may not encounter the threat. The Stay Smart Online Alert Service generally only sends alerts on those malware threats sent via spam email which are *widespread* and/or which includes subject matters which may be more likely to attract the interest of people living in Australia and therefore poses a high risk to large sections of the population that use the internet in Australia.

It is still possible, that you as a user may receive other threats via email which are not mentioned by the alert service and hence you still need to exercise caution when online.

What you can do

Subscribers should always exercise caution before clicking on links in spam email or opening attachments in email from untrusted sources. You also need to ask yourself has the “from” field on the email been changed in order to gain your trust, ie does the email falsely claim to be from a person or organisation you know and trust?

In both cases, you need to ask yourself, is the sender really who they claim to be and/or is the sender trying to fool me into doing something which could harm the security of my computer and its files?

Feedback questions – firewalls

This section is devoted responding to feedback or questions submitted by people who have subscribed to the Stay Smart Online Alert Service.

One subscriber asked whether their firewall would stop a criminal exploiting a bug in their browser software. Before answering this question, it is useful to briefly explain what browsers and firewalls do.

Web browser software includes software programs such as Microsoft Internet Explorer, Mozilla Firefox or Apple Safari. Web pages, such as the Stay Smart Online Service (www.ssoalertservice.net.au and www.staysmartonline.gov.au) are viewed through a web browser. When you view any web page through your browser over the internet, your computer makes a connection to a remote web server which allows your computer to view the web pages on the web site via your browser.

Firewalls may be separate hardware devices or a software program installed on a computer. A hardware firewall (also called an appliance firewall) is usually an external device that sits between your computer and your connection to the internet. A software firewall (also known as a personal firewall) runs directly on your computer. The software firewall is the most common type for home users.

Typically, a computer network that comprises many computers – including client and server computers would use a hardware firewall.

Software firewalls on computers include the Microsoft Windows firewall which is included as part of the Microsoft Windows XP and Vista operating systems, or separately installed firewalls such as Zone Alarm, or firewalls included with other security products sold by Symantec, Trend Micro, Sophos and other manufacturers.

While firewalls help improve the security of a computer or network, like other security technologies sometimes criminals can find ways to get around them.

If a criminal wanted to exploit a software bug in your browser in order to take control over your computer, generally, the criminal would install malicious code on a web site that was able to detect and exploit the particular software bug present on your computer. So, if for any reason you happened to visit the web site –either by going to the web site directly of your own accord, or by clicking on a link in a spam email designed to trick you to visit the web site, then often this would be enough to take over control of your computer.

Note that this type of attack may occur due to the presence of other software bugs – not just browser software bugs.

How do firewalls work?

Firewalls add a layer of protection by seeking to block unauthorised and potentially dangerous connection attempts from criminals or hackers who may wish to steal your computer data or computer's resources.

But software firewalls are not able to block *all* unauthorised and dangerous activity. For example, generally web traffic (ie , traffic which uses the protocols HTTP or HTTPS) is permitted in order to allow users to view content on web sites. For example, if you look at any web address (or URL, which stands for Universal Resource Locator), it starts with either of the following:

http://

https://

So, for example, the URL or web address for the home page of the Stay Smart Online Alert Service is:

<http://www.ssoalertservice.net.au>

This type of traffic is allowed by most firewalls. Similarly, inbound and outbound email traffic is also permitted by software firewalls. If the firewall blocked web data/traffic or email data/traffic then users would not be able to access web sites, or send and receive email.

Most software firewalls don't have the capacity to tell that the web or email traffic includes malicious code. Generally, it is only able to recognise the 'type' of traffic (such as web or email) – not whether the content is potentially harmful.

Some anti-virus software might be able to detect web or email traffic as suspicious and block the malicious code before it executes and harms your computer but generally, this may only occur if the malicious code on the remote web site or in the email attachment is already known to the anti-virus program.

So to answer the question above, in the case of software firewalls, it is very unlikely the firewall would prevent an attack that occurred as a result of exploiting a bug in browser software. But it may be effective at preventing an attack that tries to exploit a bug in other software that does not use web or email traffic protocols.

If small or medium businesses have a hardware firewall on their network, some types of hardware firewalls, including stateful or application-layer firewalls, are able to inspect the content of web or email traffic before allowing it to pass to the client computer. However, businesses should find out more about the particular type of hardware firewall they have installed and how it is configured before relying on it to detect and block this type of harmful content.

What you can do

For users that rely on software firewalls only, it is important to fix software bugs as soon as possible by downloading a software update or upgrading the software to a newer version.

Some users may question the usefulness of the software firewall if it has limited ability to block harmful web or email traffic. But when connected to the internet, **even if you are not sending or receiving email or viewing web sites, the firewall generally is able to detect and block unauthorised connection attempts that might still occur through many other ways not readily observable by users.**

For this reason every computer that is used to browse the web or read email should have its own software (personal) firewall installed. Firewalls are especially critical for users who have broadband and generally keep their computer turned on and connected to the Internet most of the time.

For small to medium size enterprises, a separate hardware firewall for the whole network may suffice, but there is no harm in also having separate software firewalls installed on each computer used by people as well (client computers).

What you can do

It is recommended that all client computers (these are those used by people) should have a software firewall installed, among other security programs. See the [Secure Computing Checklist Fact Sheet](#) for more information.

Security facts and myths

Apple Mac OS X vs Microsoft Windows

Microsoft is the world's largest developer and vendor for operating systems for people at home or in the work place (also known operating systems for client computers). Microsoft produces the Windows range of operating systems. The latest version is [Microsoft Vista](#).

Another well-known company that develops and sells operating system software for client computers is Apple which produces the Mac OS X range of operating systems. The latest version is [Apple Mac OS X Leopard](#).

People often ask are Apple Mac operating systems more secure than Microsoft Windows. There is no simple answer to this question. It depends on the criteria being considered. Some people think that just because there are fewer reports of bugs in Apple products and fewer reports of malware targeting Apple Mac products that makes Apple Mac more secure than Microsoft Windows. This is not necessarily the case.

If we compare the Apple and Microsoft operating systems (generally) there is not a lot of difference between these platforms and how they are designed, though Microsoft Windows Vista has some new features which help increase the security of the operating system and hence provide greater protection to the users' data than older versions of windows.

While there may *appear* to be more software bugs in Microsoft Windows products this is likely to be a function of how much effort criminals and bug researchers devote to finding these bugs – or whether they are interested in looking at all. Apple Mac has a very small market share compared to Microsoft Windows. Hence for many bug researchers and criminals, there is more benefit to find bugs in Windows platforms and products compared to Apple platforms.

Similarly, the number of attacks or threats that target Windows products is vastly greater compared to Apple products. This is primarily because criminals find it more beneficial to create malware that can attack a larger number of computers. This allows criminals to obtain vastly greater returns from their criminal endeavours.

Therefore, the perceived security of Windows versus Mac generally has more to do with their respective market share and the interest of criminals in obtaining most benefit for least effort.

To its credit, Microsoft recognises the threat against its software and has introduced a number of features in its operating system and applications which help users and businesses secure their computers more effectively and easily. Microsoft Vista through its User Access Control features and the Security Control Panel (the latter is also available in Windows XP) make securing the computer platform particularly easy for users.

A securely managed and updated Windows operating system is more secure than an Apple Mac that has not been securely configured nor updated.

Conversely, a securely managed and updated Apple Mac operating system is more secure than a Microsoft Windows operating system that has not been securely configured nor updated.

No online computer user can afford to be complacent about their computer's security and whether you use Apple Mac, Microsoft Windows or another operating system, users should always adopt secure online practices.

Security guides for both Microsoft Windows and Apple Mac products are available from the "Useful links".

Related articles:

<http://www.zdnet.com.au/news/security/soa/Mac-malware-volumes-spike-without-pain/0,130061744,339289766,00.htm?omnRef=1337>

<http://www.zdnet.com.au/news/security/soa/Apple-s-Leopard-hacked-in-30-seconds/0,130061744,339287733,00.htm>

http://www.infoworld.com/article/08/03/27/Gone-in-2-minutes-Mac-gets-hacked-first-in-contest_1.html

Disclaimer

This Newsletter has been prepared by AusCERT for the Department of Broadband, Communications and the Digital Economy.

The information is intended for use by home users and small to medium sized businesses and is general information only and not intended as advice and was accurate and up to date at the time of publishing. The material and information in this newsletter is not adapted to any particular person's circumstances and therefore cannot be relied upon to be of assistance in any particular case. In any important matter, you should seek professional advice relevant to your own circumstances.

The Commonwealth, AusCERT, and all other persons associated with this Newsletter accept no responsibility or liability for information either included or referred to in the Newsletter. No responsibility or liability is accepted for any damage, loss or expense incurred as a result of the information contained in the Newsletter, whether by way of negligence or otherwise.

The listing of a person or organisation in any part of this site or Newsletter does not imply any form of endorsement by the Commonwealth of the products or services provided by that person or organisation. Similarly, links to other web sites have been inserted for your convenience and do not constitute endorsement of material at those sites, or any associated organisation, product or service.

Please note that material in this Newsletter, as the case may be, includes views or recommendations of third parties, which do not necessarily reflect the views of the Commonwealth, or indicate its commitment to particular course of action. Material on this site or in this Newsletter may also include information provided by third parties. The Commonwealth cannot verify the accuracy of information that has been provided by third parties.