OUCH! | March 2014

The Monthly Security Awareness Newsletter for Computer Users

OUCH!

IN THIS ISSUE..

- Overview
- An Operating System's Life Cycle
- Protecting Yourself

The End of Windows XP

Overview

Windows XP has proven to be one of the most popular operating systems in computing history, at one point it was used on most of the computers around the world. However Windows XP is old, and all support for it from Microsoft will soon end. First released more than twelve years ago, Microsoft is scheduled to End of Life (EOL) Windows XP on April 8, 2014. This means Microsoft will no longer release any end-user updates or security patches. With approximately 25% of the world's desktop computers still running Windows XP (only Windows 7 is more popular), millions of people will be at greater risk once this happens. Keep in mind, home users are not the only ones who will be impacted as XP is still widely used in offices, industrial control systems, ATM machines, medical systems, point-of-sale terminals, and other devices. Below we describe what the risks are once Windows XP is no longer supported and steps you can take to protect yourself.

Guest Editor

Jason Fossen specializes in Microsoft Windows security at Enclave Consulting LLC, is the author of the six-day Securing Windows with the Critical Security Controls (SEC505) course at SANS, and gives away PowerShell security scripts at **http://cyber-defense.sans.org/blog/**.

An Operating System's Life Cycle

You may not know it, but your computer's operating system has a limited lifespan. The vendor who created the operating system will provide updates and patches that add new features, improve the stability and performance, and keep your system secure. The problem is that eventually the vendor will no longer support your operating system, at some point they have to focus their resources on their latest and greatest technologies. This means that once an operating system is no longer supported, the vendor will no longer release patches or updates, even when they know your computer is vulnerable and cyber criminals can hack into it. This is what is going to happen with Windows XP after April. Even though Microsoft may know your Windows XP computer is vulnerable, and cyber criminals are actively exploiting those vulnerabilities, Microsoft will stop making fixes for the problem.

The End of Windows XP

Protecting Yourself

To protect yourself you need to use an operating system that is actively supported. If you can afford it we highly recommend you purchase a new computer. Many computers running Windows XP cannot support today's newer operating systems. If you cannot afford a new computer then at least upgrade the operating system. For organizations, the transition may be less disruptive by migrating to Windows 7 instead of Windows 8 as the graphical interface in Windows 7 is similar to Windows XP. However, Windows 8 is more secure than previous versions due to significant software enhancements. In addition, there are other vendor's operating systems you can consider, such as Apple's Mac OS X. Either way, now is the time to change, you do not have much time to wait. If you simply cannot change from Windows XP before April, consider these steps.

Once Windows XP is no longer supported, the best way to protect yourself is migrate to a new operating system that is actively supported by its vendor, and ensure it is always current.

- Use your Windows XP computer only for the functionality or the applications you absolutely have to. For example, perhaps you or your organization is running an old program that only runs on XP and this is the reason you cannot upgrade. If that is the case, then do not use that computer for any other purposes, such as email or browsing the Internet.
- If you must use your Windows XP computer for browsing, stop using Internet Explorer and switch to another browser, such as Mozilla Firefox, Google Chrome, or Opera. Be sure you always keep that browser current and the vendor continues to support its use on Windows XP.
- Stop using any other built-in applications in Windows XP which open files from the Internet, such as Windows Media Player. Instead use separate applications from other vendors that are actively updated and keep them current.
- Consider using a network security service such as the free OpenDNS. Services like these protect your systems from visiting known, malicious websites. In addition, some services can detect if your computer attempts to connect to known Botnet Command and Control servers, an indicator that your system is infected.
- Make sure any security software you have installed, such as anti-virus, is still actively supported and maintained for Windows XP.

The End of Windows XP

- If your computer does not need to be connected to the Internet (for example you are using it just for word processing) then disconnect it from the network. If it must be connected to a network, be sure it is behind a firewall, and the host firewall is on blocking any traffic to it. For organizations you may want to isolate all of your Windows XP computers on a separate network, so when they are infected they do not infect the rest of your organization.
- Regularly back up data on your Windows XP computers in preparation for if or when they are infected. Keep at least one of these backups offline, such as on a disconnected USB drive. If you are forced to recover your system, strongly consider recovering to a new computer. If you recover to Windows XP again, it will most likely continue to be re-infected.

If you are using Windows XP at your organization, your employer may have additional steps you need to take. Remember, these are only a short term stop-gap measures, they are no substitute for an up-to-date, properly secured operating system. Sooner or later, you will have to migrate to a new system.

Become A Security Professional - SANS 2014

If you haven't been to SANS 2014 training in Orlando, you can't miss this on April 5-14! One of our biggest events of the year, you will have countless opportunities to develop and expand your network of security experts and friends, and learn more than you can imagine from the top instructors in the cybersecurity industry. For more information, please visit http://www.sans.org/event/sans-2014/welcome.

Resources

Microsoft EOL Announcement:	http://www.microsoft.com/en-us/windows/enterprise/endofsupport.aspx
OpenDNS:	http://www.opendns.org
Migration Guide:	http://www.zdnet.com/windows-xp-end-of-life-migration-guide-7000023800/
OUCH: Backup & Recover:	http://www.securingthehuman.org/ouch/2013#september2013

License