the Availability Digest

www.availabilitydigest.com
@availabilitydig

Windows XP Is No Longer PCI DSS Compliant

June 2014

Even though Microsoft's Windows XP operating system is still running on 25% of the world's desktop computers and PCs, Microsoft elected to end XP support on April 8, 2014. According to the Payment Card Industry (PCI) standards organization, XP systems no longer comply with the PCI Data Security Standard (DSS). Merchants still using XP-based systems to process payment cards will no longer be able to pass the PCI DSS mandatory annual compliance audit.

Requirement 6.2 of the PCI DSS states:

> "Ensure that all systems and software are protected from known vulnerabilities by installing application vendor-supplied security patches. Install critical security patches within one month of release."

Since Microsoft will no longer be providing security patches, Windows XP is, by definition, not compliant and cannot be used in payment card applications. For Internet-facing applications, XP systems will be automatically detected by ASV (Approved Scanning Vendors) scans. This will be reported as an automatic failure of the compliance audit.

Windows XP – A Haven for Hackers

In an earlier article in the *Availability Digest* on the termination of XP support,[1] we pointed out that hackers would be hoarding vulnerabilities unknown to Microsoft (so-called *zero-day exploits)* and not using them until Windows XP support ended. They then would have free reign to use these vulnerabilities to attack XP systems with no fear of the vulnerabilities being closed down by Microsoft security updates. In a recent security blog, Microsoft pointed out that the situation is far worse than this:

> "The very first month that Microsoft releases security updates for supported versions of Windows, attackers will reverse engineer those updates, find the vulnerabilities and test Windows XP to see if it shares those vulnerabilities. If it does, attackers will attempt to develop exploit code that can take advantage of those vulnerabilities on Windows XP. Since a security update will never become available for Windows XP to address these vulnerabilities, Windows XP will essentially have a "zero day" vulnerability forever.
>
> Some…are quick to point out that there are security mitigations built into Windows XP that can make it harder for such exploits to be successful. There is also anti-virus software that can help block attacks and clean up infections if they occur. The challenge here is that you'll never know, with any confidence, if the trusted computing base of the system can actually be trusted because attackers will

[1] Windows XP Retirement a Boon for Hackers, *Availability Digest*; October 2013. http://www.availabilitydigest.com/public_articles/0810/windows_xp.pdf

be armed with public knowledge of zero day exploits in Windows XP that could enable them to compromise the system and possibly run the code of their choice. Furthermore, can the system's APIs that anti-virus software uses be trusted under these circumstances?"

What Can Be Done?

Upgrade the Windows XP Systems

The only proper way to handle this situation is to upgrade Windows XP systems to Windows 7 or Windows 8 systems. Windows XP's long life has given hackers plenty of time to work around its main defense lines. Attacks have evolved and surpassed XP's ability to defend against them. Security mitigations in Windows 7 and Windows 8 are far more sophisticated.

Unfortunately, upgrading Windows XP systems can be very expensive. Subsequent versions of Windows run very poorly (or worse, not at all) on most hardware that was put in place with Windows XP. Upgrading to a supported version of Windows will probably involve upgrading the computer running it.

Given that a company is willing to bite the upgrade bullet, the first step is to identify the XP systems being used by the company. Many organizations host all or a portion of their IT environment off-site, further complicating discovery of XP.

Organizations can use vulnerability scanning to help identify all instances of XP within their environment. For instance, ControlScan is a cloud based utility that performs an internal vulnerability scan. It is a quick and easy way to discover XP within the IT infrastructure. ControlScan's scanning process is provided with a tunnel into the internal network. From there, an initial discovery scan is performed to identify all IP-addressable systems in the environment. Next, each system is scanned in turn to identify relevant attributes, services and processes. The report generated from the internal scanning process lists each IP address discovered as well as the operating system and version. This gives a clear view of where XP resides in the network.

Compensating Controls

While the ideal plan is to upgrade all XP machines to a modern operating system, some organizations simply can't allocate the necessary financial or human resources to do this. However, it is extremely important that these organizations have a game plan.

The Knowledge Base of the PCI Security Standards Council gives some guidance to a potential temporary solution known as *compensating controls*. In its Frequently Asked Question (FAQ) 1130, it raises the question:

"Are operating systems that are no longer supported by the vendor non-compliant with the PCI DSS?"

FAQ 1130 states:

"PCI DSS Requirements 6.1 and 6.2 address the need to keep systems up to date with vendor-supplied security patches in order to protect systems from known vulnerabilities. Where operating systems are no longer supported by the vendor, OEM, or developer, security patches might not be available to protect the systems from known exploits, and these requirements would not be able to be met.

However, it may be possible to implement compensating controls to address risks posed by using unsupported operating systems in order to meet the intent of the requirements. To be effective, the compensating controls must protect the system from vulnerabilities that may lead to exploit of unsupported code. … Examples of controls that may be combined to contribute to an overall compensating control include active monitoring of system logs and network traffic, properly-configured application whitelisting that permits only authenticated system files to execute, and

isolating the unsupported systems from other systems and networks. Note that these examples may complement an overall compensating control, but these examples alone would not provide sufficient mitigation.

An effective option to implement compensating controls is to enlist the services of a Managed Security Service Provider (MSSP). MSSPs specialize in delivering the technical expertise and security know-how required to meet PCI compliance requirements. They will partner with an organization to ensure that firewall settings and system configurations are secure and systems are monitored 24/7/365 for any suspicious activity.

Note that this is only a stop gap measure. There must be an action plan to remove Windows XP systems from the network as soon as is possible for your business.

Summary

Any payment systems still running the Windows XP operating system are now out of PCI DSS compliance. Without the latest security protections, your XP systems are open to all kinds of malware attacks, including stealing data. If you accept payment cards, you have something hackers want. Processing payment cards with XP systems just makes it easier to the hackers to get at them. They always go for the low-hanging fruit.

Should your organization experience a breach, you will be deemed "non-compliant," even if you were previously validated compliant. Furthermore, you will not be able to effectively pass an ASV network scan because these scans are required to automatically fail unsupported operating systems.

Perhaps an even larger problem is that 95% of ATMs worldwide are powered by Windows XP. There are 420.000 ATMs in the U.S. alone. Migrating all ATMs to a new operating system is a massive endeavor.

As complex and expensive as it may be, the security of the worldwide payment card system is dependent upon retiring all of the Windows XP systems involved in payment card processing and replacing them with modern operating systems.

Acknowledgements

Material for this article was taken from the following sources:

Knowledge Base, *PCI Security Standards Council*.
Payment Card Industry (PCI) Data Security Standard (DSS), v3.0 - Requirement 6: Develop and maintain secure systems and applications; November 2013.
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf
Windows XP Support is Ending, *PCI Security Standards Council*.
Windows XP End of Life: Why Small Merchants Must Act Now, *ComplianceGuide.org*; March 4, 2014.
No Windows XP Support, No PCI Compliance? *ComplianceGuide.org;* March 19, 2014.