SECURE WINDOWS XP WITH TRAPS

Securing Windows XP with Traps Advanced Endpoint Protection

Windows® XP end-of-life is a critical threat exposure for XP users. Security was one of the major drivers for Microsoft's decision to end support for this operating system. No doubt, the intention was to urge enterprises to upgrade their systems. In reality, however, Windows XP systems are still deployed in many organizations.

A summary of the advanced endpoint protection capabilities provided by Traps to protect unpatched Windows XP systems from exploits and malware.[1]

- Prevent exploitation of unpatched Windows XP vulnerabilities.
- Identify and block unknown malware via integration with WildFire.
- Protect legacy systems with a lightweight agent that does not rely on signatures or scanning.

Understand the Risk

Microsoft® continuously evaluates its software products to discover and patch vulnerabilities. These vulnerabilities range in severity from low to critical. A critical rating signifies a vulnerability that an attacker could exploit to gain remote code execution on a victim machine to launch a successful attack. Once patched, these vulnerabilities can no longer be exploited — assuming that users have indeed taken the trouble to deploy the patches.

Since Windows XP has reached its end-of-life, Microsoft no longer publishes any vulnerability patches for that operating system. In addition, the end-of-life for an operating system applies not only to the OS vulnerabilities, but also to the vulnerabilities of applications that run on that OS. In the case of Windows XP, the patches Microsoft releases for its Office and Internet Explorer® products cannot be applied to these products if they run on an XP endpoint.

Threat actors possess the means to reverse-engineer software patches to reveal the underlying vulnerabilities. As a result, each monthly "Patch Tuesday" may provide attackers with the knowledge of new vulnerabilities that they can utilize to compromise XP-based endpoints.

Case Study: Windows XP and Internet Explorer

An operating system is not a stand-alone product; rather, it is a platform for an application ecosystem. Following an operating system's end-of-life, the range of applications that it supports narrows significantly, especially with respect to newer and more secure versions of those applications. In the case of XP and Internet Explorer, this creates a significant security problem.

The latest version of Internet Explorer that can run on Windows XP is IE8. Following a wave of IE memory corruption vulnerabilities in 2013 and 2014, Microsoft began implementing native security provisions in Internet Explorer, beginning with IE9. As a

"Microsoft Windows XP was released almost 12 years ago, which is an eternity in technology terms. While we are proud of Windows XP's success in serving the needs of so many people for more than a decade, inevitably there is a tipping point where dated software and hardware can no longer defend against modern day threats and increasingly sophisticated cyber criminals."

Tim Rains | Director | *Microsoft Trustworthy Computing*

result, IE8 is far more exploitable than its later peers: a remote code execution vulnerability that may be natively mitigated and contained in IE10 would remain exploitable in IE8.

Prior to XP end-of-life, available security patches could have compensated for this exploitability. However, users of Windows XP systems are confined to using a version of Internet Explorer that is more vulnerable and does not receive patches for newly discovered vulnerabilities.

Case Study 2: Adobe Flash and Acrobat

In alignment with Microsoft's decision to end support for Windows XP, Adobe® ceased providing security patches to its Flash® and Acrobat® software on Windows XP following its official end-of-life. In May of 2014, Adobe updated its support website with the following guidance:[2]

"After the next official quarterly update (expected May 2014), Adobe will no longer develop versions of Acrobat or Reader for Windows XP. Also, Adobe will no longer test releases or patches on Windows XP or fix bugs specific to Windows XP."

Adobe Flash featured the highest number of newly exploited vulnerabilities in 2015. Adobe regularly issues both monthly patches and emergency fixes for discovered zero-day vulnerabilities. Neither can be applied to Flash if it runs on Windows XP. As a result, all Flash vulnerabilities discovered after May 2014 remain exposed attack surfaces for XP users.

Patch Tuesday of December 2015: Zero-Day and Critical Patches

The Patch Tuesday of December 2015 contained, among others, patches for a zero-day memory corruption vulnerability and several other critical vulnerabilities in Microsoft Office. Exploitation of these vulnerabilities enables an attacker to remotely execute code on the target user's machine. Neither of these vulnerabilities can be patched for XP users, leaving them exposed to attacks.

Palo Alto Networks Traps

Palo Alto Networks® Traps™ Advanced Endpoint Protection offers a unique approach to preventing exploits from compromising applications. Instead of focusing on the individual application vulnerabilities or the thousands of different attacks that exploit them, Traps blocks the core techniques that all exploits – including zero-day – must use to compromise applications. This is an effective strategy because all attacks that leverage unpatched software vulnerabilities rely on a small set of core techniques that change infrequently. Traps blocks these exploit techniques completely, which means that the application is no longer vulnerable despite the lack of availability of security patches.

Traps provides application-agnostic exploit prevention capabilities that apply to every user application or plugin executing in the OS ecosystem, regardless of its patching or support status. For instance, when an attacker attempts to exploit a vulnerable version of Adobe Flash or Java® that runs within Internet Explorer on Windows XP, Traps prevents the exploitation by blocking the exploit technique and terminating the process.

Traps enables you to manage your XP upgrade policy at your own pace while maintaining acceptable levels of security and compliance.

To prevent security breaches on endpoints that operate unpatchable applications and operating systems, such as Windows XP, security professionals must prevent the exploitation of known and unknown vulnerabilities associated with those applications and systems. Palo Alto Networks Traps Advanced Endpoint Protection prevents security breaches on endpoints that operate those applications and operating systems by preventing the exploitation of both known and zero-day (unknown) vulnerabilities.

To learn more about Traps, download the Traps Technical Overview white paper,[3] participate in a complimentary Ultimate Test Drive (UTD),[4] or contact your reseller to schedule a live, proof-of-concept (POC) evaluation of Traps.

1. Traps supports Windows XP x86 32-bit platforms.
2. https://helpx.adobe.com/acrobat/kb/end-of-support-acrobat-reader-on-winxp.html
3. https://www.paloaltonetworks.com/resources/whitepapers/traps-advanced-endpoint-protection-wp.html
4. http://events.paloaltonetworks.com/

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com