TRAPS FOR WINDOWS SERVER 2003

Advanced Endpoint Protection for Windows Server 2003 After End-of-Support

Microsoft® announced Windows Server® 2003 End-of-Support (EOS) on July 14, 2015. Many businesses are forced by circumstance to leave these systems in service for some time. Retiring a major enterprise component has always been a challenge for IT departments. In addition to various logistical issues, an out-of-support component is vulnerable to attack and may leave the business vulnerable to significant security and compliance risks. By employing Palo Alto Networks® Traps™ Advanced Endpoint Protection as a compensating control, businesses can keep Windows Server 2003 systems compliant and secure, even after EOS.

Security and Compliance Ramifications

Since the end-of-support for Windows Server 2003 in July 2015, Microsoft has not issued security patches to remediate vulnerabilities in that operating system. With 12 million physical servers worldwide still running Windows Server 2003,[1] a staggering number of servers may be exposed to newly discovered vulnerabilities.

For instance, a new vulnerability identified as CVE-2015-0081 was discovered in March 20152 that allowed remote attackers to execute arbitrary code via a crafted website or file. This vulnerability applied to a number of Windows® operating systems:

- Microsoft Windows Server 2003 SP2
- Windows Vista SP2
- Windows Server 2008 SP2 and R2 SP1
- Windows 7 SP1
- Windows 8
- Windows 8.1
- Windows Server 2012 Gold and R2
- Windows RT Gold and 8.1

When Microsoft issued a patch for this critical vulnerability, the patch only applied to systems that were still supported at the time.[3] Had this vulnerability been discovered five months later, Windows 2003 Server systems would not have received a security patch. Such an event would have exposed organizations that deploy that operating system in their environment to attacks.

Similarly, enterprise IT departments may reasonably assume that application vendors who have not already discontinued support for the Windows Server 2003 versions of their software will do so over time. This may result in compliance exceptions or failures.

For example, the Payment Card Industry Data Security Standard (PCI DSS) Requirement 6.2 dictates that all PCI-compliant organizations must:

> *“Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.”*[4]

Without the ability to patch new vulnerabilities, any organization that does not deploy sufficient security measures to compensate for the lack of vulnerability patches may face compliance failure.

In fact, the majority of regulatory frameworks have similar requirements; even in an unregulated, unaudited environment, an enterprise would have a difficult time defending the proposition that it did not need to maintain effective patching and software updates, especially if that was shown to be the cause of a breach.

When circumstances such as incompatible hardware, software, or infrequent downtime windows prevent organizations from migrating their servers to newer, more secure operating systems, other protective measures must be taken. Network isolation, firewalls, and host/network intrusion detection systems may all play a part, but preventing the exploitation of vulnerabilities on the endpoint itself is the last, best line of defense against advanced threats.

The Impact of Windows Server 2003 EOS

> “IT departments running unsupported software could open businesses up to elevated cybersecurity risks, hardware compatibility issues and potential compliance conflicts.”
>
> — Department of Homeland Security alert about the end-of-life for Microsoft Corp.’s Windows Server 2003

Palo Alto Networks Traps proactively and automatically prevents both exploits and malware from successfully breaching an endpoint. As its unique approach does not require prior knowledge of an attack in order to prevent it, Traps prevents both known and unknown exploits and malware, including zero-day exploits and advanced malicious executables.

Traps Advanced Endpoint Protection

Traditional endpoint security products are unable to keep up with the rapidly evolving threat landscape and are ineffective against sophisticated malware, targeted attacks and advanced persistent threats. These traditional solutions often require prior knowledge of a threat in order to prevent it or, worse, use an approach that only identifies a new threat after it has compromised the endpoint.

Many organizations today are using Traps as an effective compensating control on systems that cannot be patched. By employing Traps, businesses can not only meet regulatory requirements but far exceed compliance provisions through its automated and near-instantaneous security controls for endpoint protection.

Focus on Exploit Prevention, Not Detection

Instead of focusing on the millions of individual attacks, Palo Alto Networks Traps is designed to proactively block all attacks targeting endpoints, including unknown malware and zero-day exploits. Traps automatically blocks the core techniques that every attacker must utilize to execute an exploit, regardless of its complexity.

How Exploit Prevention Works

Many advanced threats work by placing malicious code in a seemingly innocuous data file. When the file is opened, the malicious code leverages a vulnerability

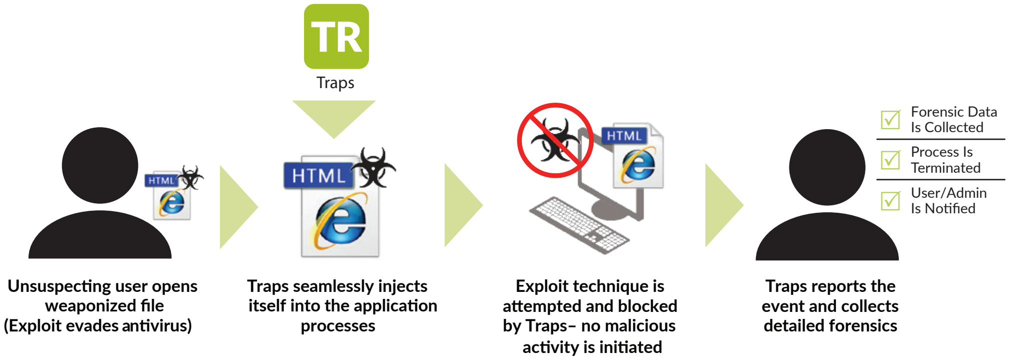
TR
Traps
HTML
Forensic Data Is Collected
Process Is Terminated
User/Admin Is Notified
Unsuspecting user opens weaponized file (Exploit evades antivirus)
Traps seamlessly injects itself into the application processes
Exploit technique is attempted and blocked by Traps– no malicious activity is initiated
Traps reports the event and collects detailed forensics

Figure 1: Traps prevents exploitation of vulnerabilities before it happens

in the native application used to view the file, and the code executes. In order to prevent this, the Traps agent injects itself into each process as it is started, as shown in Figure 1.

If an exploit attempt is made, Traps immediately blocks the attempt, terminates the process, and notifies both the user and the administrator that an attack was prevented. Throughout each event, Traps collects detailed forensics and reports this information to its administration console, the Endpoint Security Manager (ESM), resulting in better visibility and an understanding of attacks that were prevented. With Traps, endpoints are always protected, regardless of patch, signature or software update levels; plus, it requires no prior knowledge of an attack in order to prevent it.

Preventing Malicious Executables

In addition to preventing exploits, Traps employs a comprehensive approach to the prevention of malicious executables. Malicious executables can be inadvertently downloaded and run by users without their knowledge. In order to prevent executable malware, Traps focuses on core techniques, as it does for exploits embedded in data files, plus two additional methods: policy-based restrictions and integration with the WildFire™ threat intelligence cloud, as depicted in Figure 2. The multilayered malicious-executable prevention works as follows:

1. WildFire Inspection and Analysis: Traps queries the WildFire Threat Intelligence Cloud with a hash and submits any unknown .exe files to assess their standing within the global threat community.
2. Policy-Based Restrictions: Organizations can easily set up policies restricting specific execution scenarios. For example, Traps can prevent the execution of files from the Outlook temporary files directory or prevent the execution of a particular file type directly from a USB drive.
3. Malware Prevention Techniques: Traps implements technique-based mitigations that prevent attacks by blocking techniques such as thread injection.

Addressing Windows Server 2003 EOS with Traps

Prior to Traps technology, patching was the only way to provide protection from known vulnerabilities, and there was no reliable method to protect systems from unknown vulnerabilities or those with no available patch. Traps allows system operators to significantly enhance security and exceed regulatory requirements by not only eliminating known vulnerabilities but also

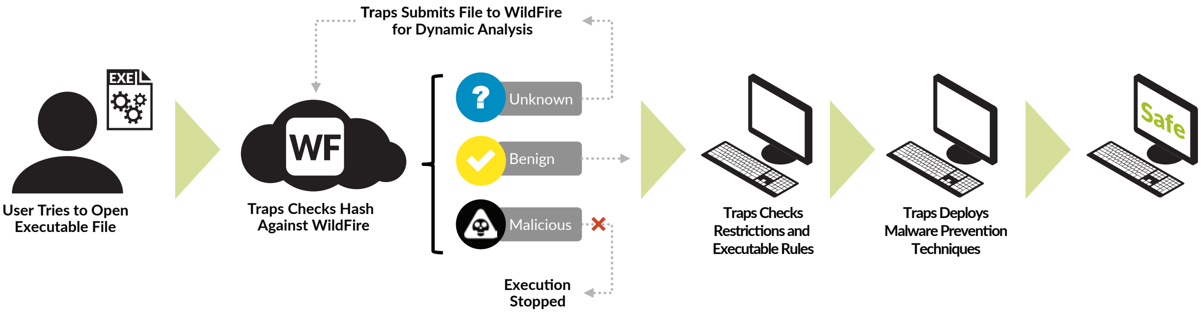
Traps Submits File to WildFire for Dynamic Analysis
EXE
WF
Unknown
Benign
Malicious
Safe
User Tries to Open Executable File
Traps Checks Hash Against WildFire
Execution Stopped
Traps Checks Restrictions and Executable Rules
Traps Deploys Malware Prevention Techniques

Figure 2: Prevention of malicious executables, a multi-tier approach

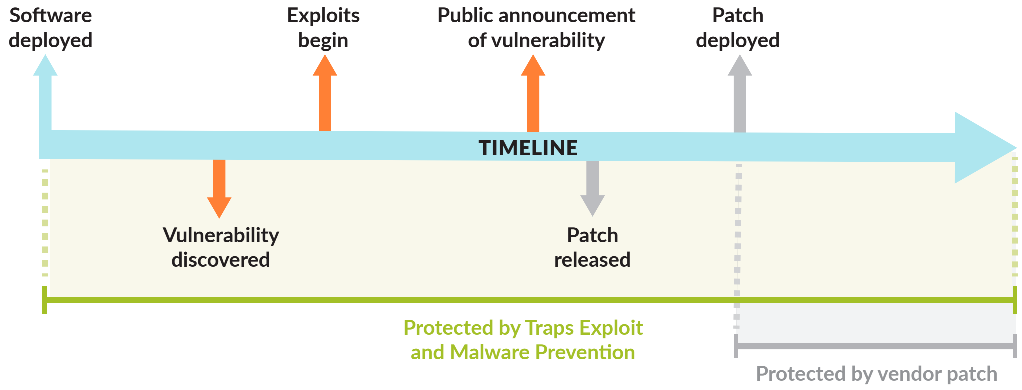
Software deployed
Exploits begin
Public announcement of vulnerability
Patch deployed
TIMELINE
Vulnerability discovered
Patch released
Protected by Traps Exploit and Malware Prevention
Protected by vendor patch

Figure 3: Traps protects endpoints regardless of availability or application of vendor patches

protecting systems from the exploitation of unknown vulnerabilities. Traps enables system and network administrators to effectively enhance their other protective measures for Windows Server 2003 systems. By preventing exploits and malware from running, Traps provides a compensating control for the vulnerabilities on these systems. Traps:

- Reduces the risk of running unsupported software by eliminating or drastically reducing entire categories of cybersecurity dangers such as malware and exploits.
- Enables regulatory compliance by providing a compensating or mitigating control to the inability to maintain properly patched systems.

Patches only protect a system after an exploit is discovered and subsequently fixed. As depicted in Figure 3, Traps protects a system before the discovery of the vulnerability, during patch development, and after patch application.

Conclusion

Windows Server 2003 has reached its end-of-life, leaving businesses without security patches that help to protect systems from harmful exploits and malware. Organizations that cannot migrate to a supported operating system in the immediate future may be exposed to increasing risks of security breaches and compliance failure associated with systems that operate Windows Server 2003. Traps Advanced Endpoint Protection provides an effective compensating control to address these security and compliance challenges.

To learn more about how Traps can help to prevent security breaches on systems that have reached their end-of-life, download the white paper titled "Securing the Unpatchable: How to Prevent Security Breaches on Endpoints When Patching Is Not an Option."

1. https://www.us-cert.gov/ncas/alerts/TA14-310A
2. http://www.cvedetails.com/cve/CVE-2015-0081/
3. https://technet.microsoft.com/library/security/ms15-020
4. https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf

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