VISA SECURITY BULLETIN

20 August 2015

WINDOWS SERVER 2003 END OF LIFE

Distribution: Acquirers, Issuers, Processors, Merchants, Agents
Who should read this: IT, Information Security, IT Support

Summary

Microsoft will no longer support or issue security fixes for Windows Server 2003 after **July 14, 2015**. This date references the end of Microsoft's "extended support" period and Microsoft will no longer offer any technical support for this platform, except for-fee custom contracts for a limited period. [1]This poses a greater risk to the data security of a company utilizing Windows Server 2003. Furthermore, as of July 15, 2015 companies using this software may no longer be in compliance with Payment Card Industry Data Security Standard (PCI DSS). It is recommended that all companies using Windows Server 2003 upgrade to Windows Server 2012 R2.

Historically, Windows Server 2003 has been vulnerable to multiple attack vectors including unauthorized privileged escalation or the execution of malicious code. In the first half of 2015 alone Microsoft identified 36 vulnerabilities attributed to Windows Server 2003, and hackers will continue to target and exploit these vulnerabilities since security patches will no longer be issued.

Another aspect of Windows Server 2003's obsolescence involves interdependent applications. Many applications in use by companies are likely to be past their rational support life and newer versions may not function with the older Windows Server 2003. This includes cloud based products from Microsoft itself as they likely require a 64-bit solution opposed to the 32-bit option which is how most Windows Server 2003 instances have been installed.

Vulnerabilities

Systems can fall out of compliance with the PCI DSS. PCI DSS Version 3.1, Requirement 6 states:

"*Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems.* ***All systems must have all appropriate software patches to protect against the exploitation and compromise of cardholder data by malicious individuals and malicious software.***"[2]

[1] Microsoft http://www.microsoft.com/en-us/server-cloud/products/windows-server-2003/
[2] Payment Card Industry Data Security Standard Version 3.1
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf

Unpatched Windows Server 2003 systems will be open to attacks through malware that cannot be detected by anti-virus or anti-malware software. Hackers will also have a greater ability to remotely access the networks utilizing Windows Server 2003. These issues have been observed in the past for Windows Server 2003 and hackers are likely to continue to exploit these known vulnerabilities.

A compromised server on the network leaves an open door for the rest of the environment to be harmed from malicious attacks. All servers should be upgraded to a currently supported operating system before the end of life date.

Operating system platforms often share application code, and malware that affects Windows Server 2012 can also harm older versions like 2003. However, while the 2012 version can be patched, there is nothing to protect Windows Server 2003.

Mitigation

The best way to protect against attacks on Windows Server 2003 is to upgrade to currently supported version of Windows Server. Windows Server 2012 R2 is the most recent platform and is recommended by Microsoft. There are also many other options including cloud based servers. [3] Once the system is migrated it is best to update all security patches and fixes immediately in order to ensure the maximum protection for your company. Ensure that the operating system is hardened to industry standards and fulfills all PCI DSS requirements as well.

Additional Resources

- Payment Card Industry Data Security Standard Version 3.1
- Microsoft.com EOS announcement

For more information, please contact Visa Risk Management: cisp@visa.com

[3] IDC White Paper *Windows Server 2003: Why You Should Get Current* http://download.microsoft.com/download/D/8/D/D8D30224-9CE4-444F-AC06-7BAFCEADBC59/Windows_Server_2003_Why_You_Should_Get_Current_IDC_Whitepaper.pdf