Australian Government
Australian Cyber Security Centre

ACSC
AUSTRALIAN CYBER SECURITY CENTRE
PROTECT

February 2015

End of Support for Microsoft Windows Server 2003

Introduction

1. The Australian Signals Directorate's *Strategies to Mitigate Targeted Cyber Intrusions* ranks timely patching of operating system vulnerabilities and using the latest suitable operating system version as the third most effective strategy to mitigate targeted cyber intrusions.

2. On 14 July 2015, Microsoft will end support for Microsoft Windows Server 2003. After this date, organisations will no longer receive patches for security vulnerabilities identified in this product. Adversaries may use these unpatched security vulnerabilities to target systems, increasing the likelihood of a successful targeted cyber intrusion.

Intended audience

3. This advice is intended for organisations unable to upgrade from Microsoft Windows Server 2003 by 14 July 2015.

Scope

4. This document is separated into:

   a. mitigation strategies for organisations operating an entire Microsoft Windows Server 2003 server fleet

   b. mitigation strategies for organisations that have limited remaining Microsoft Windows Server 2003 server deployments to support legacy business applications.

Recommendations

5. ASD strongly recommends organisations using Microsoft Windows Server 2003 upgrade to a newer supported operating system such as Microsoft Windows Server 2012 R2 by 14 July 2015.

6. Organisations unable to upgrade to a newer supported operating system by 14 July 2015 should review the risk assessment for their ICT environment and implement additional controls identified below to reduce their risk exposure.

Operating an entire fleet

7. Organisations continuing to operate an entire Microsoft Windows Server 2003 server fleet beyond 14 July 2015 should implement the following host-based controls:

   a. **Mitigation Strategy #1:** Implement an application whitelisting solution, such as Software Restriction Policies (SRP). Application whitelisting, when implemented appropriately, can detect and prevent malicious code execution, network propagation and data exfiltration by an adversary.

b. **Mitigation Strategy #2:** For unsupported native applications either upgrade to supported versions or, if this is not possible, consider removing the application or using alternative applications to achieve similar business functionality. Each application upgraded, removed or replaced with an alternative generally reduces the attack surface of servers and can assist in preventing malicious code execution.

c. **Mitigation Strategy #3:** Negotiate an extended support arrangement with Microsoft for the provision of patches for security vulnerabilities. Whilst an extended support arrangement will not address all security vulnerabilities disclosed for legacy Microsoft applications, it will assist in reducing the attack surface of servers.

d. **Mitigation Strategy #4:** Avoid using privileged accounts on servers for day-to-day activities. Instead, a low privileged account should be used for all non-administrative activities and privileged accounts used strictly for administrative activities. Servers will soon be at a higher risk of being compromised due to unpatched vulnerabilities, and lack additional security functionality of newer Microsoft Windows Server versions to protect privileged account credentials from being captured by an adversary and used to propagate throughout a network.

e. **Mitigation Strategy #7:** Implement Microsoft's Enhanced Mitigation Experience Toolkit (EMET). Implementing EMET for applications that commonly interact with data from untrusted sources can reduce the risk of successful malicious code execution as well as assisting in the identification of such attempts.

f. **Mitigation Strategies #12 and #13:** Implement a third party software-based application firewall that performs both inbound and outbound filtering of traffic. A software-based application firewall can assist in detecting and preventing malicious code execution, network propagation and data exfiltration by an adversary.

g. **Mitigation Strategies #21, #24, #25 and #27:** Apply basic hardening, where possible, to servers, software and all accounts including the use of a strong passphrase policy. Applying basic hardening principles, such as disabling unneeded functionality or common intrusion vectors such as autorun, SMB and NetBIOS services, can assist in preventing malicious code execution and network propagation by an adversary.

h. **Mitigation Strategies #22 and #30:** Ensure antivirus applications continue to be supported by vendors. If support ceases from a vendor, switch to an alternative vendor that continues to offer support. The use of antivirus applications can assist in detecting and preventing malicious code execution.

8. In addition to the above host-based controls, the following controls can be implemented to reduce the likelihood of malicious code reaching servers in the first place. These include:

a. **Mitigation Strategy #23:** Prevent servers from directly accessing and being directly accessible from the Internet. By preventing servers from directly accessing and being directly accessible from the Internet, their exposure to untrusted content can be reduced. In cases where patches need to be applied to servers or their applications these should be downloaded from the Internet via alternative means and transferred by appropriate means to the server.

b. **Mitigation Strategy #26:** Prevent users from connecting portable media to servers. By preventing portable media being connected to servers, the ability to introduce malicious code to vulnerable servers will be reduced.

Operating a limited deployment

9. Organisations continuing to operate a limited Microsoft Windows Server 2003 deployment beyond 14 July 2015 to support legacy business applications should consider implementing the following controls:

    a. **Mitigation Strategy #10:** Isolate servers from other non-essential network services. This can reduce the risk of an adversary using a compromised server to propagate throughout a network and access other network resources.

    b. **Mitigation Strategy #14:** Virtualise servers and required applications from within a vendor-supported operating system e.g. Microsoft Windows Server 2012 R2. Using virtualised environments can hamper an adversary's ability to extend their reach beyond the virtualised environment and propagate to other network resources.

    c. **Mitigation Strategy #23:** Prevent servers from directly accessing and being directly accessible from the Internet. By preventing servers from directly accessing and being directly accessible from the Internet, their exposure to untrusted content can be reduced. In cases where patches need to be applied to servers or their applications these should be downloaded from the Internet via alternative means and transferred by appropriate means to the server.

Additional considerations

10. Independent of how Microsoft Windows Server 2003 servers are operated by organisations beyond 14 July 2015, additional controls can be implemented to assist in the identification and remediation of cyber intrusions. These include:

    a. **Mitigation Strategies #15 and #16:** Implement a robust centralised logging and auditing framework to capture and analyse both server and network-based events. An appropriate auditing framework within an organisation can assist in identifying individual servers that may have been compromised as well as helping to tailor incident response measures to remove infected servers from an organisation's network.

Further Information

11. This document complements the advice listed in ASD's *Strategies to Mitigate Targeted Cyber Intrusions*. This publication is available at http://www.asd.gov.au.

12. Further information on patching operating systems can be found in ASD's Protect publication *Assessing Security Vulnerabilities and Patches*. This document, and additional ASD Protect publications, can be found at http://www.asd.gov.au/publications/index.htm.

Contact Details

13. Australian government customers with questions regarding this advice should contact ASD Advice and Assistance by emailing asd.assist@defence.gov.au or by calling 1300 CYBER1 (1300 292 371).

14. Australian businesses or other private sector organisations seeking further information should contact CERT Australia by emailing info@cert.gov.au or by calling 1300 172 499.