Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

End of Support for Microsoft Windows Server 2008 and Windows Server 2008 R2

JUNE 2020

Introduction

The ***Strategies to Mitigate Cyber Security Incidents*** ranks timely patching of security vulnerabilities, as well as using the latest operating system versions, as essential mitigation strategies in preventing cyber security incidents.

On 14 January 2020, Microsoft ended support for Microsoft Windows Server 2008 and Windows Server 2008 R2. As such, organisations no longer receive patches for security vulnerabilities identified in these products. Subsequently, adversaries may use these unpatched security vulnerabilities to target Microsoft Windows Server 2008 and Windows Server 2008 R2 servers.

Organisations using Microsoft Windows Server 2008 and Windows Server 2008 R2 should upgrade to the latest version of Microsoft Windows Server 2016 or Windows Server 2019 to continue receiving patches for security vulnerabilities, while also benefiting from security improvements in the newer operating systems. Organisations yet to upgrade to a newer supported operating system should review their risk assessments and begin planning for the implementation of mitigation strategies to reduce their risk exposure – noting there will still be an overall increase in risk exposure until such a time that Microsoft Windows Server 2008 and Windows Server 2008 R2 servers are upgraded.

The advice in this publication is intended for organisations unable to upgrade from Microsoft Windows Server 2008 and Windows Server 2008 R2. The advice is separated into mitigation strategies for organisations operating a fleet of Microsoft Windows Server 2008 and Windows Server 2008 R2 servers, and mitigation strategies for organisations that have a limited number of Microsoft Windows Server 2008 and Windows Server 2008 R2 servers in order to support legacy business applications.

Operating a fleet of Microsoft Windows Server 2008 and Windows Server 2008 R2 servers

Organisations continuing to operate a fleet of Microsoft Windows Server 2008 and Windows Server 2008 R2 servers beyond the end of support date should implement the following mitigation strategies:

- Implement application control, such as Microsoft's AppLocker. Application control, when implemented appropriately, can detect and prevent malicious code execution and network propagation attempts by an adversary.
- 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 unsupported application upgraded, removed or replaced with a vendor-supported alternative generally reduces the attack surface of servers and can assist in preventing malicious code execution.

- Negotiate an Extended Security Update (ESU) arrangement with Microsoft for the provision of patches for security vulnerabilities in Microsoft Windows Server 2008 and Windows Server 2008 R2[1]. Whilst an ESU arrangement will not address all security vulnerabilities disclosed for legacy Microsoft applications, it will assist in reducing the attack surface of servers. Note, if choosing to migrate Microsoft Windows Server 2008 and Windows Server 2008 R2 servers from on-premises to Azure, organisations will receive three years of patches for free instead of requiring an ESU arrangement with Microsoft.
- Ensure that privileged account credentials are not entered into Microsoft Windows Server 2008 and Windows Server 2008 R2 servers (e.g. to administer workstations, other servers or applications within an organisation's network). Instead, a vendor-supported operating system should be used for these activities, and a low privileged account used for all other non-administrative activities. Microsoft Windows Server 2008 and Windows Server 2008 R2 servers will be at a higher risk of being compromised due to unpatched security 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.
- 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.
- Implement a third party software-based application firewall that performs both inbound and outbound filtering of network traffic. A software-based application firewall can assist in detecting and preventing malicious code execution, network propagation and data exfiltration by an adversary.
- Apply basic hardening, where possible, to operating systems, applications and user accounts. 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.
- 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.

In addition to the above mitigation strategies, a number of mitigation strategies can be implemented to reduce the likelihood of malicious code reaching Microsoft Windows Server 2008 and Windows Server 2008 R2 servers in the first place. These include:

- Implement automated dynamic analysis of email and web content in a sandbox to detect suspicious behaviour. By analysing data from untrusted sources for suspicious activity upon simulated user interaction, malicious code can be identified and blocked from reaching vulnerable Microsoft Windows Server 2008 and Windows Server 2008 R2 servers.
- Implement email and web content filtering of incoming and outgoing data to only allow approved file types. By controlling the types of data that reach Microsoft Windows Server 2008 and Windows Server 2008 R2 servers, organisations can reduce the likelihood of malicious code execution as well as identify the source of such attempts.
- Prevent users from connecting removable media to Microsoft Windows Server 2008 and Windows Server 2008 R2 servers. As Microsoft Windows Server 2008 and Windows Server 2008 R2 servers are more susceptible to exploitation, data transfers to such servers should be controlled via an organisation's ICT service desk to reduce the likelihood of malicious code execution and data exfiltration.

[1] https://azure.microsoft.com/mediahandler/files/resourcefiles/end-of-support-sql-server-and-windows-server-2008-and-2008-r2/Windows_Server_2008_SQL_Server_2008_End_of_Support_Security_Brief.pdf

Operating a limited number of Microsoft Windows Server 2008 and Windows Server 2008 R2 servers

Organisations continuing to operate a limited number of Microsoft Windows Server 2008 and Windows Server 2008 R2 servers beyond the end of support date in order to support legacy business applications should implement the following mitigation strategies:

- Isolate Microsoft Windows Server 2008 and Windows Server 2008 R2 servers from other non-essential network resources. This can reduce the risk of an adversary using compromised Microsoft Windows Server 2008 and Windows Server 2008 R2 servers to propagate throughout a network and access other network resources.
- Virtualise access to Microsoft Windows Server 2008 and Windows Server 2008 R2 operating environments and required applications from within a vendor-supported operating system. Using virtualised environments can hamper an adversary's ability to extend their reach beyond the virtualised environment and propagate to other network resources.
- Prevent Microsoft Windows Server 2008 and Windows Server 2008 R2 servers from directly accessing, and being directly accessible from, the internet. As legacy business applications are likely to operate in a local stand-alone mode, or only require access over an organisation's intranet, restricting access from Microsoft Windows Server 2008 and Windows Server 2008 R2 servers to and from the internet can reduce the risk of such servers being directly compromised by an adversary.

Additional considerations

Independent of how Microsoft Windows Server 2008 and Windows Server 2008 R2 servers are operated by organisations, organisations should 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 can be found in the Australian Cyber Security Centre's ***Windows Event Logging and Forwarding*** publication[2].

Further information

The ***Australian Government Information Security Manual*** (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. It can be found at https://www.cyber.gov.au/acsc/view-all-content/ism.

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of strategies can be found at https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents.

Advice from Microsoft on Microsoft Windows Server 2008 and Windows Server 2008 R2 End of Life support can be found at https://support.microsoft.com/en-au/help/4456235/end-of-support-for-windows-server-2008-and-windows-server-2008-r2.

[2] https://www.cyber.gov.au/acsc/view-all-content/publications/windows-event-logging-and-forwarding

Advice from Microsoft on getting and installing Extended Security Updates for eligible devices is available at https://techcommunity.microsoft.com/t5/windows-it-pro-blog/how-to-get-extended-security-updates-for-eligible-windows/ba-p/917807/page/3.

Advice from Microsoft on migrating Microsoft Windows Server 2008 and Windows Server 2008 R2 servers to Azure is available at https://www.microsoft.com/en-au/cloud-platform/windows-server-2008.

Contact details

If you have any questions regarding this guidance you can contact us via 1300 CYBER1 (1300 292 371) or https://www.cyber.gov.au/acsc/contact.