Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

# End of Support for Microsoft Windows and Microsoft Windows Server

**First published**: November 2019
**Last updated:** March 2024

## Introduction

The *Strategies to Mitigate Cyber Security Incidents* ranks timely patching of vulnerabilities, as well as using the latest or previous version of the latest operating system release, as essential to contributing to the prevention of cyber security incidents.

Under Microsoft's Windows lifecycle policy, support for Microsoft Windows and Microsoft Windows Server varies depending on the release (e.g. Microsoft Windows 11), edition (e.g. Enterprise) and version (e.g. 23H2) of operating systems. Notably, following the expiration of the specified servicing timeline, organisations will no longer receive patches for vulnerabilities identified in these products. Subsequently, malicious actors may increasingly target workstations or servers running these unsupported versions of Microsoft Windows and Microsoft Windows Server.

Organisations using unsupported versions of Microsoft Windows or Microsoft Windows Server should upgrade to supported versions to continue receiving patches for vulnerabilities, while also benefiting from security improvements in the newer supported versions. Organisations yet to upgrade to supported versions of Microsoft Windows or Microsoft Windows Server 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 unsupported versions are upgraded to supported versions.

The advice in this publication is intended for organisations unable to upgrade unsupported versions of Microsoft Windows or Microsoft Windows Server on workstations or servers, herein referred to as unsupported workstations or servers.

## Mitigation strategies for unsupported workstations or servers

Organisations continuing to operate unsupported workstations or servers beyond their specified servicing timeline should implement the following mitigation strategies:

- Implement application control, such as Microsoft's AppLocker. Application control, when implemented appropriately, can assist in preventing malicious code execution and network propagation attempts by malicious actors.
- For unsupported native applications, either upgrade to supported versions or, if this is not possible, consider removing the applications 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 workstations and servers, and can assist in preventing malicious code execution.

- Ensure that privileged account credentials are not entered into unsupported workstations or servers (e.g. to administer applications, workstations or servers) as they will be at higher risk of capture by malicious actors. Instead, a supported workstation or server should be used for system administration activities.

- If supported, 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 malicious actors.

- 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 malicious actors.

- 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 unsupported workstations or 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 unsupported workstations or 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 unsupported workstations or 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 and other devices to unsupported workstations or servers as they are more susceptible to exploitation. Instead, data transfers to unsupported workstations or servers should be controlled via an organisation's ICT service desk to reduce the likelihood of malicious code execution and data exfiltration.

- Isolate unsupported workstations or servers from other workstations, servers and non-essential network resources. If possible, consider running an unsupported workstation or server within its own virtual machine that can only communicate with a host running a supported operating system. This can reduce the risk of malicious actors using a compromised unsupported workstation or server to propagate throughout a network and access other workstations, servers or network resources.

- Prevent unsupported workstations or servers from directly accessing, and being directly accessible from, the internet. Restricting access for unsupported workstations or servers to and from the internet can reduce the risk of them being directly compromised by malicious actors.

# Additional considerations

Independent of how unsupported workstations and servers are operated by organisations, organisations should implement a robust centralised logging and auditing framework to capture and analyse both computer, server and network-based events. In doing so, an appropriate auditing framework within an organisation can assist in identifying

individual workstations or servers that may have been compromised, as well as helping to tailor cyber security incident response activities to remove infected workstations or servers from an organisation's network.

# Further information

The *Information Security Manual* is a cyber security framework that organisations can apply to protect their systems and data from cyber threats. The advice in the *Strategies to Mitigate Cyber Security Incidents*, along with its Essential Eight, complements this framework.

Further information on Microsoft Windows 11 releases is available from Microsoft.

Further information on Microsoft Windows 10 releases is available from Microsoft.

Further information on Microsoft Windows Server releases is available from Microsoft.

# Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).

**Disclaimer**

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.



## For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)


**Australian Government**

**Australian Signals Directorate**