Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

End of Support for Microsoft Windows 10

NOVEMBER 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.

Under Microsoft's current servicing model, support for Microsoft Windows 10 will end between 18 to 30 months after release depending on the version and edition being used. At such a time, organisations will no longer receive patches for security vulnerabilities identified in these products. Subsequently, adversaries may use these unpatched security vulnerabilities to target workstations running unsupported versions of Microsoft Windows 10.

Organisations using unsupported versions of Microsoft Windows 10 should upgrade to the latest version to continue receiving patches for security vulnerabilities, while also benefiting from security improvements in the newer operating system. Organisations yet to upgrade to a supported version 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 the version of Microsoft Windows 10 being used is upgraded.

A list of upcoming end of support dates for Microsoft Windows 10 versions is shown below, versions of Microsoft Windows 10 that no longer receive any support are not shown.

Version	Home, Pro & Pro Education Editions	Enterprise and Education Editions
Microsoft Windows 10 version 20H2	10 May 2022	09 May 2023
Microsoft Windows 10 version 2004	14 December 2021	14 December 2021
Microsoft Windows 10 version 1909	11 May 2021	10 May 2022
Microsoft Windows 10 version 1903	8 December 2020	8 December 2020
Microsoft Windows 10 version 1809	10 November 2020	11 May 2021
Microsoft Windows 10 version 1803	12 November 2019	11 May 2021

Mitigation strategies for unsupported versions

Organisations continuing to operate Microsoft Windows 10 workstations 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 workstations and can assist in preventing malicious code execution.
- Ensure that privileged account credentials are not entered into workstations using unsupported versions of Microsoft Windows 10 (e.g. to administer other workstations, servers or applications within an organisation's network). Instead, a supported version of Microsoft Windows 10 should be used for these activities, and a low privileged account used for all other non-administrative activities. Workstations running unsupported versions of Microsoft Windows 10 will be at a higher risk of being compromised due to unpatched security vulnerabilities, and lack additional security functionality of newer versions of Microsoft Windows 10.
- 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, a number of mitigation strategies can be implemented to reduce the likelihood of malicious code reaching workstations running unsupported versions of Microsoft Windows 10 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 workstations running unsupported versions of Microsoft Windows 10.
- 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 workstations running unsupported versions of Microsoft Windows 10, organisations can reduce the likelihood of malicious code execution as well as identify sources of such attempts.
- Prevent users from connecting removable media to workstations running unsupported versions of Microsoft Windows 10. As workstations running unsupported versions of Microsoft Windows 10 are more susceptible to exploitation, data transfers to such workstations should be controlled via an organisation's ICT service desk to reduce the likelihood of malicious code execution and data exfiltration.
- Isolate workstations running unsupported versions of Microsoft Windows 10 from other workstations and non-essential network resources. This can reduce the risk of an adversary using a compromised workstation to propagate throughout a network and access other workstations and network resources.
- Prevent workstations running unsupported versions of Microsoft Windows 10 from directly accessing, and being directly accessible from, the internet. Restricting access from such workstations to and from the internet can reduce the risk of such workstations being directly compromised by an adversary.

Additional considerations

Independent of how workstations running Microsoft Windows 10 are operated by organisations, organisations should implement a robust centralised logging and auditing framework to capture and analyse both computer and network-

based events. An appropriate auditing framework within an organisation can assist in identifying individual workstations that may have been compromised as well as helping to tailor incident response measures to remove infected workstations from an organisation's network. Further information can be found in the Australian Cyber Security Centre's ***Windows Event Logging and Forwarding*** publication[1].

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 the new Microsoft Windows 10 lifecycle can be found at:

- https://support.microsoft.com/en-au/help/13853/windows-lifecycle-fact-sheet
- https://docs.microsoft.com/en-au/windows/deployment/update/waas-servicing-differences.

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.

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