Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

End of Support for Microsoft Windows 7

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 7. As such, organisations no longer receive patches for security vulnerabilities identified in this product. Subsequently, adversaries may use these unpatched security vulnerabilities to target Microsoft Windows 7 workstations.

Organisations using Microsoft Windows 7 should upgrade to the latest version of Microsoft Windows 10 to continue receiving patches for security vulnerabilities, while also benefiting from security improvements in the newer operating system. 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 7 is upgraded.

The advice in this publication is intended for organisations unable to upgrade from Microsoft Windows 7. The advice is separated into mitigation strategies for organisations operating an entire Microsoft Windows 7 fleet and mitigation strategies for organisations that have limited Microsoft Windows 7 deployments in order to support legacy business applications.

Operating a fleet of Microsoft Windows 7 workstations

Organisations continuing to operate a fleet of Microsoft Windows 7 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.
- Negotiate an Extended Security Update (ESU) arrangement with Microsoft for the provision of patches for security vulnerabilities in Microsoft Windows 7. Whilst an ESU arrangement will not address all security vulnerabilities disclosed for legacy Microsoft applications, it will assist in reducing the attack surface of workstations.

- Ensure that privileged account credentials are not entered into Microsoft Windows 7 workstations (e.g. to administer other workstations, 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 7 workstations will be at a higher risk of being compromised due to unpatched security vulnerabilities, and lack additional security functionality of newer Microsoft Windows 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 7 workstations 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 7 workstations.
- 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 7 workstations, 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 7 workstations. As Microsoft Windows 7 workstations 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.

Operating a limited number of Microsoft Windows 7 workstations

Organisations continuing to operate a limited number of Microsoft Windows 7 workstations beyond the end of support date in order to support legacy business applications should implement the following mitigation strategies:

- Isolate Microsoft Windows 7 workstations from other workstations and non-essential network resources. This can reduce the risk of an adversary using a compromised Microsoft Windows 7 workstation to propagate throughout a network and access other workstations and network resources.
- Virtualise access to Microsoft Windows 7 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 workstations and network resources.
- Prevent Microsoft Windows 7 workstations 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 7 workstations to and from the internet can reduce the risk of such workstations being directly compromised by an adversary.

Additional considerations

Independent of how Microsoft Windows 7 workstations 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 Microsoft Windows 7 End of Life support can be found at https://www.microsoft.com/en-au/microsoft-365/windows/end-of-windows-7-support.

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.

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