November 2016

End of Support for Microsoft Windows Vista and Microsoft Office 2007

Introduction

1. The Australian Signals Directorate's *Strategies to Mitigate Targeted Cyber Intrusions* ranks timely patching of extreme risk security vulnerabilities in applications and operating systems, as well as using the latest suitable versions of applications and operating systems, as highly effective mitigation strategies for targeted cyber intrusions.

2. In April 2017 and October 2017, Microsoft will end extended support for Microsoft Windows Vista[1] and Microsoft Office 2007[2] respectively. After these dates, organisations will no longer receive patches for security vulnerabilities identified in these products. 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 Vista and/or Microsoft Office 2007 by Microsoft's end of extended support dates.

Scope

4. This document is separated into:

   a. mitigation strategies for organisations operating an entire Microsoft Windows Vista and/or Microsoft Office 2007 fleet

   b. mitigation strategies for organisations that have limited Microsoft Windows Vista and/or Microsoft Office 2007 deployments to support legacy business applications.

Recommendations

5. ASD recommends organisations using Microsoft Windows Vista and/or Microsoft Office 2007 upgrade to a vendor-supported operating system such as Microsoft Windows 10 Anniversary Edition by April 2017 and office suite such as Microsoft Office 2016 by October 2017.

6. Organisations yet to upgrade to a newer supported operating system and office suite by these dates should review risk assessments for their networks and begin planning for the implementation of additional mitigation strategies to reduce their risk exposure.

7. Implementing the mitigation strategies from this document on a vendor-supported operating system will result in a much stronger security posture than implementing the mitigation strategies on a legacy non vendor-supported operating system.

[1] https://support.microsoft.com/en-au/lifecycle/search/?c2=11732
[2] https://support.microsoft.com/en-au/lifecycle/search/?p1=8753

Operating an entire fleet

8. Organisations continuing to operate an entire Microsoft Windows Vista and/or Microsoft Office 2007 fleet beyond the end of extended support dates should implement the following mitigation strategies:

    a. Implement an application whitelisting solution, such as Microsoft's AppLocker. Application whitelisting, when implemented appropriately, can detect and prevent malicious code execution, network propagation and data exfiltration by an adversary.

    b. 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 workstations and can assist in preventing malicious code execution.

    c. Negotiate an extended support arrangement with Microsoft for the provision of patches for security vulnerabilities in Microsoft Windows Vista, Microsoft Office 2007 and Internet Explorer 9. 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 workstations.

    d. Ensure that privileged account credentials are not entered into Microsoft Windows Vista workstations e.g. to administer the workstation or other applications or systems 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 Vista 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.

    e. 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. 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. Apply basic hardening, where possible, to operating systems, applications and user accounts. 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. 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.

9. In addition to the above mitigation strategies, a number of mitigation strategies can be implemented to reduce the likelihood of malicious code reaching workstations in the first place. These include:

    a. 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 workstations.

b. 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, organisations can reduce the likelihood of malicious code execution and as well as identifying the source of any such attempts.

c. Prevent users from connecting portable media to workstations. Portable media infected with malicious code can result in the exploitation of vulnerable workstations. As Microsoft Windows Vista 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 deployment

10. Organisations continuing to operate a limited Microsoft Windows Vista and/or Microsoft Office 2007 deployment beyond the end of extended support dates to support legacy business applications should consider implementing the following mitigation strategies:

    a. Isolate Microsoft Windows Vista workstations from other workstations and non-essential network services. This can reduce the risk of an adversary using a compromised workstation to propagate throughout a network and access other network resources.

    b. Virtualise access to Microsoft Windows Vista 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.

    c. Prevent Microsoft Windows Vista 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 such workstations to and from the Internet can reduce the risk of workstations being directly compromised by an adversary or having data exfiltrated by an adversary should any workstation become compromised.

Additional considerations

11. Independent of how Microsoft Windows Vista and Microsoft Office 2007 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

12. 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/infosec/mitigationstrategies.htm.

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

Contact details

14. 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).

15. Australian businesses or other private sector organisations with questions regarding this advice should contact CERT Australia by emailing info@cert.gov.au or by calling 1300 172 499.