Guidance

Obsolete platforms guidance

Published

Contents

This guidance is intended to help organisations that are unable to fully migrate away from obsolete or unsupported platforms prior to the ‘end of support’ date by providing short-term mitigation advice. Obsolete platforms will no longer receive security updates from the developer, and will lack many of the security technologies that are present in newer versions of the product (if available). This guidance does not provide a risk-free way of continuing to use these obsolete products, but will help reduce the risks of doing so.

When a product is no longer supported by its developer, there are limits on the mitigations that will be effective in protecting against new threats that will emerge. Over time new vulnerabilities will be discovered and will be exploitable by relatively low-skilled attackers. No combination of the mitigations described within this guidance will fully mitigate the risks posed by a vulnerable operating system remaining in active use. The principles apply to any software (client or server operating system, or end user application) which is approaching the end of its support period.

1. Migrate away from obsolete software

It is vital that all organisations only use software products which are supported by the vendor, and that plans be made to migrate from older products as the end of support period is reached. After these dates there will be no security patches published for these products.

No new deployments of such obsolete technologies should be undertaken, and

organisations should limit investment on obsolete technologies (for example, no new applications which require legacy operating systems should be deployed).

The upgrade of high risk end user devices and servers should be prioritised. These include systems used for corporate remote access, as they will be subject to greater physical threat and be more susceptible to network-borne attacks. Devices that can access more sensitive information or services, including personal data, should also be prioritised.

Where it proves impossible to complete the migration before the end of the support period, additional mitigations will be needed to help reduce the likelihood of compromise and to minimise the harm should a compromise occur. These are discussed below.

2. Short-term mitigations

Weaknesses that are found in unsupported products will remain unpatched and will be exploitable by relatively low skilled attackers. There are two types of mitigations that can be used to reduce the risk:

- Reduce the likelihood and scope for compromise by preventing the devices from accessing untrusted content - effectively making it hard for malicious content to reach the device and exploit it.
- Reduce the impact of compromise by preventing access to sensitive data or services from vulnerable devices, so even if the devices are compromised, the damage will be minimised.

An effective mitigations plan will likely require a combination of these approaches.

3. Mitigations to reduce the likelihood of compromise

Exploits based on malicious data can only be successful if the data can actually reach an unpatched product. If untrusted data is prevented from reaching a system, then the likelihood of malicious content reaching the vulnerable system is lowered, and so the risk from malicious content is reduced.

Routes by which malicious data could reach obsolete software include email, web browsing, file shares, network ports, and removable media. It is recommended that these routes be reduced for vulnerable devices. Servers should not be used for end-user activities (such as email or web browsing), and data flows to unpatched servers should be carefully considered and reduced wherever possible.

Data and files sourced from the Internet should be treated as untrusted even if originating from a known third party. Data retrieved from enterprise storage services should also be treated as untrusted if its source was external.

3.1 Mitigation: Prevent access to untrusted services

Implement technical controls to prevent access to external untrusted services from vulnerable systems. This should include preventing access to external email and preventing the device from browsing the internet via a native web browser (indirect access e.g. via a thin client is possible). These controls will not be effective if they are not technically enforced.

By preventing access via email and the web browser to untrusted content and services, two of the most likely attack vectors for client systems are removed.

3.2 Mitigation: Reduce use of untrusted services

As it may not be possible to fully prevent access to all external untrusted services without adversely affecting business functions, it is possible to slightly reduce the risk of compromise by ensuring that access to content, particularly active content or media, is done by a manual action. This intentional action can reduce the risk of “drive-by download” attacks.

Suggested approaches for legacy versions of Windows are provided below.

There is no way to completely mitigate the exposure of an unpatched web browser to malicious web content, beyond blocking access to it entirely. However the risk can be lowered by blocking access to rich web content, scripting and by using of a gateway that scans all incoming content for malicious content.

3.3 Mitigation: Prevent access to removable media

Access to removable media should be prevented as it can be used to transport untrusted content. It is also important to consider devices such as smartphones and tablets, which can be used to transfer media, and, if compromised, can also launch attacks against devices they are connected to. Access to removable media and any connected devices can be controlled through numerous third party products and through some BIOS configuration pages.

3.4 Mitigation: Convert obsolete client systems to thin clients

Convert any obsolete machines to thin client devices and use them only as an access mechanism to trusted internal services, such as a VDI environment. By using them as a thin client it is possible to avoid the need for the device to directly process untrusted content. Web browsing, for example, can be performed via a VDI environment running a patched modern browser, and business productivity applications can be accessed in a similar way. This allows the remote session to run supported, patched software, even if the client device used to access services cannot. The remote system should be configured to prevent transfer of data back to the client device using features such as clipboard sharing and file transfers.

This mitigation can be strengthened by ensuring the client devices are in a separate Active Directory forest to the VDI images and other enterprise services.

3.5 Mitigation: Remove network access for remote workers

When an obsolete device is connected to untrusted networks via its network interfaces, it is directly exposed to external network-borne attacks. The only technical mitigation available would be to disable/remove all network access from the device, effectively making them stand-alone devices. This is clearly only possible if the applications on this device do not require access to network services.

Alternatively, the device could be connected to a physically or logically separate network which only has those legacy applications and their required services on it, but this will enable malware to spread very quickly should this network be compromised.

3.6 Mitigation: Remove remote access from obsolete client devices

Some remote access solutions include end user device posture checks on incoming connections. It may be possible to use these posture checks to enforce barring of obsolete client devices from remotely accessing corporate systems. This will reduce the risk of the enterprise network being exposed to a compromised unpatched device. This control would only help protect the enterprise network from attack; it does not protect any data stored or cached on a client device.

Where organisations expose some of their internal services to unmanaged end user devices (BYOD) this control is also likely to be useful to ensure that users do not remotely access organisational information from devices known to be vulnerable.

3.7 Mitigation: Remove unneeded services from obsolete servers

Obsolete servers should be checked to ensure that the services they offer are minimal. Those services which are not required to support the business function of the server should be turned off. Wherever possible, migrate required services from obsolete servers to modern, supported, servers. It is recommended that obsolete servers are not used to provide VDI services, or other remote desktop facilities, where there is any expectation of separation between users or where the remote desktop / VDI solution is being used to provide security separation within a network.

3.8 Mitigation: Remove remote access to obsolete servers and services

Obsolete servers are likely to have unpatched vulnerabilities, and fewer exploit mitigations to help prevent those vulnerabilities from being exploited. To reduce the attack surface, these services should not be exposed to untrusted networks such as the Internet. Intrusion prevention services and application firewalls can be used to help defend against attacks, as can protocol breaks through the use of reverse proxy servers.

4. Mitigations to reduce the impact of compromise

An unpatched end user device that is directly exposed to malicious content is likely to result in successful compromise. The impact of compromise can be reduced by controlling access to enterprise services hosting sensitive data and improving the ability to detect attacks.

4.1 Mitigation: Remove access to services from obsolete clients

The level of access granted to obsolete devices into an enterprise environment should be restricted to only those functions which are absolutely critical. Implementation of this mitigation will require network separation and zoning controls to be used.

4.2 Mitigation: Re-image/wipe devices regularly to attempt to remove any resident malware

Obsolete platforms will be more likely to contain malware from a previous compromise. Therefore they should be regularly re-imaged to remove any malware present. However it is important to remember that this will only temporarily sanitise the devices as the same exploit which the malware used initially to gain a presence on the platform will continue to work after the device has been re-imaged, so the device will still be vulnerable to attack.

4.3 Mitigation: Treat obsolete systems as unmanaged or untrusted

Where obsolete client devices continue to be used within an organisation, it is strongly recommended that they be treated as untrusted devices and given constrained access as a result. CESG BYOD guidance provides guidance on designing a suitable network architecture to provide this type of separation. Obsolete servers should be treated by the wider enterprise as being untrusted, and data and services they offer should be handled accordingly.

4.4 Mitigation: Network zoning

By zoning the network it is possible to reduce the ability for malware to spread laterally through an enterprise. The traffic flows between zones should be well-defined, providing the ability to block and prevent unauthorised communications, such as those made by malware trying to reach its command and control systems.

It must be assumed that successful attacks against obsolete or unpatched operating systems are likely to be able to subvert the controls provided by any software firewall in that operating system.

Appropriate internet gateway mitigations, such as using an authenticated outbound proxy, will help ensure that internet-bound traffic flows are authorised. Also by using website reputation filtering it is possible to reduce the likelihood users can reach malicious sites.

Obsolete servers should be placed into network zones that minimise the traffic which can reach them. Access to those zones should only be granted to clients with a need to communicate with servers in those zones.

4.5 Mitigation: Protective monitoring capability improvement

For the times in which the enterprise environment is at higher risk (e.g. when running obsolete software) it is especially important to ensure an effective and proactive protective monitoring capability is in place. Many organisations often have the ability to record security events but do not proactively alert or take action based upon those events.

4.6 Mitigation: Anti-malware and intrusion detection products

Products such as antivirus, host-based and network-based intrusion detection systems can be used and will continue to offer some benefits in detecting malicious code. Their effectiveness may be reduced as the products may not be updated when running on an unsupported operating system and signatures may not be tuned to detect attacks targeted

at obsolete systems.

4.7 Mitigation: Incident response

Timely response to security critical events becomes increasingly important if obsolete and vulnerable software is present within the enterprise environment. Actions to contain and eradicate the compromise should be swift to try and reduce any compromise spreading.

All incidents should be recorded and reported to the appropriate CERT.

5. Additional Considerations

5.1 Third party connections

If third party organisations use their own devices within or to connect in to your environment (for example, suppliers that manage services within your enterprise environment) it is important to understand whether they are running obsolete and vulnerable software which could pose a risk to your systems - and to take action to address such risks.

6. Specific recommendations for Microsoft products

The 'end of support' dates for products such as Windows XP, Office 2003, Windows Server 2003, Exchange 2003 and Sharepoint 2003 should be understood, and effective plans made for migration to alternative, supported products.

6.1 Mitigation: Office 2003 file types

With regard to Office 2003 no longer being supported after 8th April 2014, an effective, albeit restrictive, control is to prevent the file types that Office 2003 can open being transferred through gateways. Any internet email gateways and proxies should filter these file types if the organisation still uses Office 2003 after this date.

The Windows registry could be edited so that vulnerable Office components and Media Players are not registered as the default applications for the relevant file types. This ensures that files can only be opened by a user intentionally initiating the action from within the product. Removing the registry key settings identified by the following PowerShell script will achieve this:

```
Get-ChildItem HKLM:\Software\Classes -Recurse -ErrorAction SilentlyContinue | foreach {
```

```
  if($_ -match "\\shell\\[a-zA-Z0-9]*\\command$")
  {
   $path = $_
   #Search for filetypes associated with Windows Media Player
   if($path.GetValue('') -match "wmplayer.exe")
   {
      Write-Host -ForegroundColor Green $path
   }
   #Search for filetypes associated with Office 2003
   if($path.GetValue('') -match "Microsoft Office\\Office11")
   {
      Write-Host -ForegroundColor Green $path
   }
  }
}
```

Note that appropriate testing should be carried out before implementing this across the estate. If third party products handle some files in the list that are produced by the PowerShell script above, then those file extensions could be removed from the list to ensure that only file types still associated with those products are disabled.

6.2 Mitigation: Deploy EMET

Some of the older Microsoft platforms still have a supported version of the EMET available. This tool makes it harder for some vulnerabilities in the platform to be exploited, but will not completely prevent attacks.

6.3 Mitigation: Custom Support Agreement (CSA)

The Custom Support Agreement is a paid for service available to customers who have a Microsoft Premier Support agreement. Under such an agreement Microsoft will supply both Critical and Important security updates, Important Updates are available at an additional fee. The types of updates that will be available via the CSA will be similar to those that would be available to a product in ‘extended support’. Once a product goes into extended support there is no guarantee that all future security vulnerabilities will be addressed and so it should not be seen as a long term alternative to full migration to a modern supported operating system.

Legal information

This guidance is issued by CESG, the UK's National Technical Authority on Information Assurance. One of the roles of CESG is to provide advice to UK government entities and organisations providing services to UK government. The guidance found here is provided

and intended for use by this audience. It is provided 'as-is' as an example of how specific requirements could be met. It should be used to help inform risk management decisions on the use of the products described, but it should not be used for procurement decisions; it is not intended to be exhaustive, it does not act as an endorsement of any particular product or technology, and it is not tailored to individual needs. It is not a replacement for independent, specialist advice. Users should ensure that they take appropriate technical and legal advice in using this and other guidance published by CESG. This guidance is provided without any warranty of any kind, whether express or implied. It is provided without any representation as to the accuracy, completeness, integrity, content, quality, or fitness for purpose of all or any part of it. CESG cannot, then, accept any liability whatsoever for any loss or damage suffered or any costs incurred by any person as a result of, or arising from, either the disclosure of this guidance to you, or your subsequent use of it.