BRITISH COLUMBIA | Ministry of Citizens' Services

Information Security Guidelines for Aging Systems

January 2020

CIRMO CSD ES ICT OCIO PSD RPD SBC

As technology is advancing and vendors develop new applications and software, they will eventually stop providing important security updates and support for the older technology. Vendors will issue end-of-support notices for the applications and software that they plan to retire. The *System Acquisition, Development and Maintenance Security Standard* requires that the software and systems used for government business to have vendor support and that security updates and patches are applied in a timely manner. Therefore, it is critical to start planning to migrate systems that are nearing the end of vendor support to newer vendor supported solutions once these notices are issued.

Ministries and organizations managing IM/IT infrastructure on behalf of government must comply with the *System Acquisition, Development and Maintenance Security Standard.* System owners should develop a migration roadmap for their systems and communicate this information to executives and decision-makers to get the required budget and resources for the migration of these systems before the vendor support for them ends.

The OCIO recognizes that ministries may find themselves out of compliance with the *System Acquisition, Development and Maintenance Security Standard* particularly in the case where they discover a system they were not aware of. This guideline has been developed to help ministries address the security risks created by obsolete systems they have failed to identify and migrate to vendor supported software products.

Note: This guidance does **not** condone use of obsolete products. Its purpose is to help ministries reduce the security risks of obsolete products as they work expediently to address them.

Exemptions from the System Acquisition, Development and Maintenance Security Standard from are required to use obsolete systems. Complete a Security Threat and Risk Assessment and provide a mitigation plan with timelines to migrate to a vendor supported system along with the exemption request.

Why is it important to address systems before they become obsolete?

One of the problems of using obsolete products is that product developers will no longer provide security updates for them. This increases the likelihood of threat actors exploiting unpatched vulnerabilities in the product. The other problem is that the latest security controls are not present in or can't be applied to older systems. This increases the number of vulnerabilities and the success rate of exploitation of BC Government systems. It also makes detecting and stopping of any exploitation more difficult.

In combination, these two problems make the likelihood of high-impact security incidents significantly higher. Malware can easily exploit unpatched vulnerabilities and quickly spread from one vulnerable system to another across the SPAN BC network. This may have extremely adverse consequences and high financial costs for BC Government. In this way, obsolete systems in one Ministry may put all of government at risk.

In addition, when a product is no longer supported by its developer, there are limits on the mitigations that will be effective in protecting against new emerging threats. Over time, new vulnerabilities that can be exploited will continue to be discovered in the obsolete product by threat actors. No amount of mitigating controls will completely remove the risks posed by obsolete products remaining in active use, for example, Windows XP. Therefore, as organizations prepare their mitigating safeguards, they should also work in parallel on migrating the obsolete systems to a vendor supported system as soon as possible.

Migrate to a vendor supported system

Ministries must have an action plan and allocate resources in a timely manner to migrate away from software products nearing end of vendor support prior to support end date. After these dates, there will be no security patches published for obsolete products, and any vulnerabilities found in these products will permanently remain exploitable by attackers.

To migrate from software scheduled to be obsolete, consider the following:

- No new deployments or new investments should be made in technologies scheduled to be obsolete (e.g., no new applications should be developed or deployed using an older version of JRE plugin).
- Upgrades of high-risk end user devices and servers should be prioritized, especially devices that can access more sensitive information or services, including personal data.

Steps to take to minimize the security risks from using obsolete systems in the interim:

1. Apply short-term mitigations

Weaknesses and vulnerabilities that are found in unsupported systems will remain unpatched and can be easily exploited by attackers. There are two types of mitigations that can be used to reduce the risk:

a) reduce the *likelihood* of compromise by preventing access of untrusted content on vulnerable devices making it hard to exploit the device vulnerabilities; and
b) 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 minimized).

Vulnerable devices could be compromised by malicious content in emails, websites and files through sharing, network ports, removable media and installation of unauthorized software and applications. Where possible, these avenues of compromise should be limited on the vulnerable device and more discriminating configuration policies should be applied. Data and files sourced from the Internet should be treated as untrusted even if they appear to originate from a known third party.

To reduce the security risks of obsolete systems, consider the following:

- Where possible, prevent or reduce the use of untrusted services on vulnerable devices and servers. As it may not be feasible to fully prevent access to external untrusted sources of content 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 (e.g., browser plugins), is either disabled or done only by a manual action.
- Where possible, restrict access to obsolete systems by using virtual containers or thin clients. This will limit the exposure of the obsolete systems from other vulnerabilities that may exist on the devices used to access them.
- Limit the access to services and particularly to sensitive information to a minimum number of users and devices. Where possible, remove or reduce remote access to the obsolete systems.
- Apply network zoning and segmentation policies to limit the impact of a potential compromise on the organization.
- Ensure an effective and proactive protective monitoring capability is in place, anti-malware, firewalls, web application firewalls, host-based and network-based intrusion detection systems are operating in real-time and configured to treat the content associated with obsolete systems more aggressively than other systems.
- Ensure an incident response plan is in place and can be implemented immediately if the obsolete system is compromised. Timely and effective response is critical to containing the incident and to limit the impact of the compromise.

2. Third-party connections

If you find yourself running an obsolete system, you need to understand how other ministries and organizations may also rely on that system and the impacts to them. It is your responsibility to inform the organizations that the system is obsolete and include all the stakeholders in your mitigation plans and activities.

If you are working with external third-party organizations who may have access to your network and resources (e.g., contractors, suppliers), it is important to know if they are using obsolete and vulnerable systems to access your information resources as those could also pose a risk to your environment. Work with them to mitigate such risks.

3. Extended support agreements

In some cases, vendors and developers may offer a paid subscription service to continue to provide critical and important security updates and patches for a limited period past the end-of-support date for the system. While this is an interim mitigation option, it does not provide long term benefits as these services are often limited in scope and are usually quite expensive. A migration to a vendor supported solution is the main strategy to reduce security risks.