Obsolete products

CANADIAN CENTRE FOR CYBER SECURITY

March 2023 | ITSAP.00.095

Organizations like yours make a significant investment in procuring IT assets required to enable your operations. Most of these assets (both hardware and software) have a limited lifespan as they become out of date or eventually become obsolete. Although these products may remain in working condition, they may unknowingly be putting your organization at risk if they continue to be used. It's a good practice to discontinue the use of technologies once they are obsolete. However, realistically, organizations will need time to upgrade or replace IT assets. This document offers some guidance on how to minimize risks as your organization transitions away from obsolete products.

What are obsolete products?

The International Electrotechnical Commission (IEC) defines obsolete products as no longer produced by the manufacturer in accordance with the original specification [IEC 62402]. Product vendors make a strategic decision to sunset a product to intentionally phase it out or retire it. Vendors may also abandon product lines if they become too expensive to run or maintain. As such, they will stop providing support (security updates, bug fixes, and feature upgrades) for older versions of their products.

What are the risks with obsolete products?

It's commonplace for most organizations to use their IT assets until they're out of date or long past the recommended replacement cycles. As long as out of date or legacy assets receive vendor support, there's minimal risks to their continued use. However, prolonged use of obsolete assets with no clear plan to upgrade or replace them puts your organization at a greater risk of compromise. Some of the risks include:

Security vulnerabilities. Obsolete products that no longer receive security updates are more likely to be vulnerable to cyber attacks. New found issues or vulnerabilities in these products will remain unpatched and become potential attack vectors for threat actors to exploit.

System crashes and unavailability. Eventually, obsolete software will no longer run on new hardware and will become incompatible with newer operating systems. This could lead to instability, poor performance or improper operation of your system which could result in crashes and system downtime. The cost to your organization may be disruption to your business operations and result in decreased revenue.

Increased financial costs. Obsolete products or systems may be more expensive to maintain beyond their sunset period. Premiums may need to be paid to the product vendor (or other third party vendors) to maintain support for the organizational context. Additional in-house resources may be required.

Legal and regulatory compliance risks. Using obsolete or unsupported products may increase your compliance risks that you may not even be aware of. Failure to transition from unsupported software or legacy systems may result in regulatory penalties, lawsuits, financial liability or business suspension.

Obsolete products in industrial control systems (ICS) and operational technology (OT)

ICS and OT systems are designed and built with reliability as one of the most essential requirements. This is key as both systems play an important role in the support and management of critical infrastructures. The lifecycle of ICS/OT systems are much longer compared to any other systems and, as their components age, they become increasingly difficult to repair or replace. Also, obsolete systems are unlikely to be supported by the manufacturers and/or suppliers. As such, operators and owners of ICS/OT systems need to take a proactive approach and plan for the replacement of these systems and their components well before they become obsolete. If a replacement strategy is not feasible, then a minimum set of mitigation measures should be in place to protect these systems. A good obsolescence mitigation plan should include the following:

- Backup and spares policies that account for non-availability of replacement products due to market conditions.
- Programs to ensure sufficient in-house resources are available and trained to rebuild systems to a known-good configuration.
- Best practices for how to secure products requiring internet/cloud/wireless connectivity.
- Approved vetting process to select vendors that provide proactive lifecycle planning, especially Mean Time Between Failures (MTBF) estimates as well as advance notice of End of Support (EOS) dates.
- Required security controls to implement before the EOS date to protect the ICS/OT networks. For more information, see Security considerations for industrial control systems (ITSAP.00.050) and Protect your operational technology (ITSAP.00.051).

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada

Obsolete products

CANADIAN CENTRE FOR CYBER SECURITY

March 2023 | ITSAP.00.095

How to manage the risks from obsolete products

The first and most important step to managing your risks from obsolete products is to **inventory** the IT assets (hardware and software) running on your network. Take careful stock of all assets and document their type and version. The next step is to **identify** the assets that are no longer supported by a vendor or have reached their end-of-life. Consider implementing the following **short-term mitigation measures** to minimize your risks of potential cyber security attacks and reduce the impact of a compromise.

- ☐ **Disconnect obsolete devices** from your network that are no longer in use and are not required operationally.
- ☐ **Implement network security zones** to control and restrict access and data communication flows to and from obsolete components. Segment networks to divide your network into several smaller components to make it more difficult for ransomware to spread across the entire network. For more information, see Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089).
- ☐ **Use preventative security tools such as anti-malware, anti-virus, and firewalls, as well as a host intrusion detection system (HIDS)** to reduce the risks associated with malicious intrusions (e.g. malware, spyware, and unauthorized users). Be aware that since obsolete systems are unlikely to receive updates, the efficacy of these security tools may be reduced.
- ☐ **Restrict connections of obsolete components to untrusted networks such as the Internet**. If this is not possible, block access to rich web content and media (ie. macros and browser plugins). Enable vulnerability scanning of your network edge to detect incoming malicious traffic. This minimizes the chance of malware reaching obsolete components on your system.
- ☐ **Prevent access to removable storage devices** like USB thumb drives, which can be used to transport malicious content to obsolete devices. Block access to removable storage media by disabling USB ports or deny access via group policy.
- ☐ **Check what services are running on obsolete servers** and disconnect or disable non-essential services. Required services should be moved to supported servers or cloud services.
- ☐ **Set up logging, monitoring and auditing** of obsolete components on your system. This will allow you to detect what types of attacks are being attempted against them and implement proactive mitigation measures. For more information, see Network security logging and monitoring (ITSAP.80.085) and Network security auditing (ITSAP.80.086).
- ☐ **Develop an incident response plan** that includes the processes, procedures, and documentation on how your organization detects, responds to, and recovers from cyber attacks.
- ☐ **Remove and sanitize data from decommissioned devices or storage media** so it can't be recovered or accessed. Ensure you backup your data before sanitizing a device.
- ☐ **Dispose of hardware and software at the end of their lifecycle**. In some cases, physical destruction of the device or media (along with proper sanitization) is the best option to ensure sensitive data is made inaccessible . For more information, see Sanitization and disposal of electronic devices (ITSAP.40.006).
- ☐ **Periodically sanitize obsolete products that are still in use** to remove possible malware that may have been implanted. This is a temporary measure as the device will remain vulnerable if the attack route to it is not mitigated.

Managing obsolescence long-term

Here are some long-term strategies to help your organization better manage the risks from obsolete products.

- Establish an IT asset management program (ITAM) to track, monitor and maintain your IT assets throughout their lifecycle from procurement to disposal. Leverage the use of ITAM tools to efficiently manage your assets.
- Develop a transition plan for all your IT assets from the time the product is procured to the end of its support period. The plan should cover the process to update, upgrade or replace the product, and training for your staff on how to operate newer systems.
- Consider purchasing lifetime product support when procuring new hardware or licensing new software.
- Select products with open data formats where possible. This could minimize potential issues with accessing or migrating data that is locked-in or has proprietary data formats.

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada