Risks of using discontinued software

ENISA warns about the risks of using discontinued software, not only because of the lack of support from the manufacturer, but also from third parties, like manufacturers of anti-malware or other kind of software, or computer peripherals. This will lead in persistent exposure to vulnerabilities and lack of possibility to update peripherals or third party applications.

1 Introduction

Frequently, cyber-security incidents are caused by unpatched software systems which are vulnerabile to widely accessible exploits. This is the case even when the patches are available in the moment of the attack. There are cases when such attacks are perpetrated before the patchs are distributed, either as consequence of the exploitation of a zero day vulnerability or because the vulnerability was known but the solution to the problem was still pending and a turn-around solution was lacking.

To prevent the spread of such incidents the European Union Agency for Network and Infromation Security (ENISA) calls upon:

- **CERTs** to identify and classify vulnerabilities and attack patterns, and define counter-measures;
- **Manufacturers** to adhere to “security by design” principles during software development and also to implement a predictable product patching lifecycle;
- **Users’ vigilance**; one should be able to detect abnormal behaviour of their system, allow the quick detection of the threat, promptly install published patches and follow configuration guidelines.

Installation of patches presumes their availability. They need to be developed by the manufacturer of the system. Normally commercial manufacturers produce patches during the life cycle of the product, and commit themselves to continue generating them for some years after the end of the product’s distribution in the market. At the end of this extended life cycle, the manufacturer discontinues its support for product maintenance, and stops any activity around it, once it is considered that customers have had enough time to upgrade their platforms to newer products.

This risk scenario is particularly relevant in the case of legacy software in industrial control systems (ICS) and SCADA, because those ICS are implemented using proprietary software with relatively limited number of licenses distributed, and for this reason normally immune to most widely known attacks targeting standard software. The problem is that in the last years the trend in cybercrime isthe targetted attacks, based on attack patterns and tools specially tailored for one organisation or propietary software. Energy, nuclear and financial Critical Infrastructures systems have experienced well known incidents, and for this reason special care has to be taken with them.

2 Risks associated with the use of discontinued software

Using discontinued software implies exposure to the following risks:

- **End-users** will be unable to check the integrity of the software, because Signing certificates may be expired, i.e. not-valid. This will be the case only if the last original distribution was signed by the manufacturer.
    - Being unable to check the integrity of the software package could expose the user to malware.

- Potentially infected systems may spread the infection over the whole network.
- Also, this could lead to non-compliance with security policies.

- Loss of product support by the discontinued **software manufacturer** could potentially lead to the following:
  - Users of discontinued systems will not benefit from security updates or notices;
  - New Vulnerabilities will no longer be collected, reported and analysed, thus new security patches will not be released; and then in effect the discontinued software may stay exposed to each such vulnerability, forever… as if it were a 0-day attack vector.
- Lack of support from **third party software** and hardware manufacturers could lead to unavailability to use the platform, e.g.:
  - unknown bugs may stop discontinued software from running;
  - Incompatibility of old Operating Systems with new devices[1], unavailability of drivers for new versions of peripherals may prevent users from upgrading or replacing used or broken devices;
  - Suspension of support of existing devices on the discontinued platform may result on impossibility to continue using the device in case of failure;
  - Incompatibility issues of new applications or newer versions due to termination of support by third party manufacturers also for the discontinued platform software may prevent customers from upgrading or patching also third party software.
  - This may be particularly critical in case of unavailability of updated versions of anti-virus and anti-malware solutions.

3 ENISA's recommendations

1. **IT Managers** should always keep systems up to date with the latest security patches. Discontinued software should be considered a high security risk for critical IT components and should be mitigated by migrating to newer solutions or other platforms. In the case of Critical Infrastructures Information systems, the risk of exposure may be extended to citizens, and thus the responsibility of IT managers is larger.
2. **Manufacturers** should make sure that they provide enough time for migration. During this phase, ENISA strongly recommends the use of advance notices and also an in-depth analysis of the expected impact on users' security after the product will be discontinued.
3. **Users** should make sure that they are aware and understand the security risk they are exposing themselves to by continuing to use obsolete software.

[1] Printers, scanners, webcams, drivers, etc.