



Software has an expiry date

How to react to End-of-Life announcements

Software vendors regularly make announcements that certain versions of software will no longer be supported after a particular date. Such dates are known as End-of-Life (sometimes shortened to EOL). Remain alert about announcements of the End-of-Life of software and react to these as soon as possible.

After the End-of-Life, software is no longer supported and can therefore not be considered to be secure. This means that it is important to update systems as soon as possible and replace unsupported software.

It is important for companies to be aware of the software in use so that the impact of an End-of-Life announcement can quickly be estimated. When the list of the software in use is expanded to include any dependencies between the various different applications, a more comprehensive picture can be achieved concerning the impact of a migration path.

Target audience

This fact sheet is aimed at software and system administrators. If you have outsourced the support of your workplaces and servers, then you should consult your vendors about how you can best handle this subject.

Key facts

- » Vendors regularly make announcements that a particular product will no longer be supported. Such dates are known as End-of-Life.
- » A software package in which a vulnerability is discovered after End-of-Life, will remain vulnerable to attacks.
- » When an End-of-Life announcement is made, you should start with the upgrade process as soon as possible.
- » Upgrading may lead to compatibility problems with other programs. Therefore you should start to plan, test and implement upgrades as soon as possible.
- » There are alternatives available for many types of software, possibly from other vendors.
- » Some systems, such as medical or industrial machinery, cannot be upgraded: alternative measures exist for these, but they require intensive administration.

What is End-of-Life of software?

End-of-Life is the date after which a particular software product will no longer receive any updates. Vendors regularly announce End-of-Life of software. This may involve operating systems, but it may also involve other types of software and firmware. An End-of-Life announcement will often be made long in advance. The vendor will no longer provide updates for this product after that date.

For example, an announcement was made some time ago about the end of support for Windows XP¹. Announcements were also made for other software, for example Windows Server 2003², Ubuntu distributions³ or Adobe software⁴.

This factsheet was compiled in collaboration with Microsoft, the Radiocommunications Agency, the Tax and Customs Administration and the Dutch Banks.

¹ See also the Fact sheet 'Stop using Windows XP' (2013-2014): <https://www.ncsc.nl/english/services/expertise-advice/knowledge-sharing/factsheets/factsheet-stop-using-windows-xp.html>.

² Windows Server 2003 announcement: <http://www.microsoft.com/en-us/server-cloud/products/windows-server-2003/>

³ Ubuntu release end-of-life: <http://www.ubuntu.com/info/release-end-of-life>

⁴ Adobe Lifecycle Policy: <https://www.adobe.com/support/products/enterprise/eol/>

Programming errors are found in many software packages after their release. Some of those errors are limited to the working of the system, while other types of errors are possibly security risks. The latter errors may, for example, allow malicious parties to hack into the computer system. The software vendor will repair these errors in subsequent versions of the software, but systems using the current version will therefore be vulnerable in the meantime. For this reason, vendors regularly issue updates for their software. Installing the updates fixes the vulnerabilities known at that time, which are the result of those programming errors.

Newly discovered errors will often not be fixed after the End-of-Life. Antivirus software can only resist a portion of the attacks on these vulnerabilities. The same applies to a firewall or an Intrusion Detection/Prevention System (IDS/IPS): it may well resist a portion of the attacks, but by no means all of them.

What could happen?

Software that is still being used after its End-of-Life will become increasingly vulnerable to attacks. An attack on a vulnerable system can be made in a number of different ways, depending on the type of software. It may, for example, take place when visiting an infected website or when opening a malicious e-mail attachment, but many different paths of attack are possible. Every computer that is connected with the outside world in one way or another can, in principle, become infected. Such a connection may be direct, via a network or internet connection, but it may also be indirect via an infected USB stick or via other devices that are connected to the same network, such as printers.

An attacker who infects a computer with malicious software will then often have access to all the information on that computer, and from there the attacker can continue the attack to all connected computers and/or devices in the network. The attacker can then see, change or remove any information he wishes. The computer is then no longer suitable for carrying out confidential actions or financial transactions; such transactions can be seen and changed by the attacker.

What can you do?

The most important measure to prevent that a computer with unsupported software remains vulnerable, is to replace such software early with software that is supported.

It is advisable to keep a comprehensive list of the software in use. Maintain an updated list of End-of-Life announcements concerning software on the basis of this list. Such announcements are often made on the vendor's website or sent via a newsletter. If an announcement is made, start planning migration paths as soon as possible.

Software vendors often make announcements well in advance concerning software packages that will no longer be supported, and they will themselves offer solutions or alternatives. Besides new versions of the software, alternatives are commonly offered by other

vendors as well. Should a system contain software that can not be replaced, complete replacement of the system should be considered.

There are also risks involved in upgrading software. An upgrade may lead to other dependent software no longer functioning properly. This may involve, for example, software that is dependent on an older version of the operating system. Interdependencies may also exist between different programs, for example in the way in which information is exchanged between programs. Your software vendor will be able to provide you with further information about this.

Software Lifecycle Management

Software Lifecycle Management (SLM) is a continuous process that plays in the purchase, installation, use and phasing out of software. SLM that is well thought through provides good predictability of software administration and reduces the possibility of exploitation of vulnerabilities.

SLM comprises a number of different phases that involve the entire lifecycle of software. The different phases are the purchase phase, the implementation and configuration phase, the production phase, including any change process, the maintenance phase and finally the phasing out of the software. At the end of the lifetime of the software, this cycle starts again from the beginning.

End-of-Life plays a role in different phases of SLM:

- » In the choice of **software to be purchased**, take into account which process the vendor uses for fixing errors and vulnerabilities.
- » Install updates as soon as possible during the **production phase**. Give security updates the highest priority in order to remedy vulnerabilities in the software.
- » Follow the announcements made by the vendor during the **maintenance phase**. They will announce updates and publish an End-of-Life. If you receive an End-of-Life announcement while you are still using the software in question, then you should replace the software with a new version or an alternative in order to prevent your organisation from becoming vulnerable after the End-of-Life.

Migrating software may be a substantial project. It is important to look at the dependencies of software packages, and then to find out whether these will still work with the new versions. It may be that new alternatives will then need to be sought out or even that hardware may need to be replaced. Employees will often need to be given training in order to be able to use the new software.

The amount of time software migration paths will take may vary depending on the nature of the software and the size of the

organisation. In the case of smaller packages, this may take less than a month, but in the case of larger software packages, such as operating systems, this may take between six and twelve months. Your IT department and vendors are important partners in this kind of migration path: involve them at every stage of the process.

Alternatives to upgrading

The NCSC strongly advises all computer users and system administrators with unsupported software to change over to other supported software. However, this may not be possible for all systems. Operating and management systems for medical or industrial devices often use outdated software. Their importance warrant extra attention for their security. Alternative measures should be taken, where necessary, to reduce security risks for these devices.

Smartphones and tablets

Mobile devices, such as smartphones and tablets, also have their own operating systems, which regularly require updating. Manufacturers regularly announce new versions and thereby provide information concerning which devices will or will not be continued to be supported. In the case of mobile devices, of which the operating system will no longer be updated, then the same advice applies as for computers: replace these as soon as possible.

In relation to software on mobile devices (apps), the advice also applies that updates should be installed as soon as possible. Such updates are issued regularly and are announced via the app stores or on the device itself.

Unfortunately, in the case of apps that are no longer supported, usually no End-of-Life announcement is made. In such cases we advise that the vendor's website should be consulted regularly and, in case of doubt, contact the vendor.

If it is impossible to update or replace a computer with outdated software, then there are several measures that can be taken in order to reduce the chance of infection or being hacked:

- » It is important to limit connection with the outside world as much as possible. Ideally this will mean that such a computer should not have a connection with the internet, should not be connected to a network and that no external media, such as USB drives, should be used.
- » However, if it does appear necessary to connect the computer to the office network or to the internet, then this connection should only be used for strictly necessary actions, or the system should be placed in a segmented part of the network.
- » Install updates for the other installed software, if these are available.
- » Switch off unnecessary network services in the computer.
- » Only allow the computer to be used with local accounts; do not log into company or administrators' accounts.
- » Actively monitor the network connection with an IDS or an IPS (Intrusion Detection/Prevention System).
- » If the use of external media, such as USB drives, is necessary, format these for use on a secure (therefore different) computer. Regularly scan the external media in use for viruses on a secure (therefore different) computer, for example every time before use.

Finally:

Just as with other products, software has a limited lifetime. The vendor will periodically issue updates during the lifetime of a software package in order to update the software. It is important to install such updates as soon as possible. In the case of much software, its life is not limitless. Vendors will stop supplying a particular line of products, or they will provide a new alternative. An End-of-Life announcement will then be made concerning the old product. Ensure that there is comprehensive list of the software in use, so that announcements will be noticed and migration paths can be started early.

How to proceed:

- 1 Ensure that there is a comprehensive list of the software in use on all systems.
- 2 Map the dependencies of and between the software and systems in use. Make sure that this list is continually kept up-to-date.
- 3 When purchasing software, choose products that are still being maintained. Base your choice, for example, on the compatibility with other software in use.
- 4 Keep aware of announcements issued by the software vendors in order to remain well informed about any relevant End-of-Life.
- 5 Start a migration path early with the assistance of your IT department and your IT vendors in order to be able to switch over from software, concerning which an End-of-Life announcement has been made.
- 6 Does your network include computers that cannot be upgraded, despite the disadvantages involved? Then you should take additional measures in order to close off these computers as far as possible from the local network, the internet and potential attackers.



Publication of **National Cyber Security Centre**

Turfmarkt 147 | 2511 DP The Hague | The Netherlands

P.O. Box 117 | 2501 CC The Hague | The Netherlands

www.ncsc.nl/english | info@ncsc.nl | T +31 70-751 55 55

Publication No.: FS-2015- o | No rights may be derived from this information.

