T2021_20 Understanding Software Patches and Updates (30th November 2021)

What are Software Patches and Updates?

A software patch commonly known as a fix, is a small piece of software that addresses security vulnerabilities within a program or product. Software vendors may choose to release updates to fix performance bugs, as well as to provide enhanced features.

How do you know what software updates you need to install?

When software updates become available, they are usually placed on the vendors website for download by users. It is advised to install updates as soon as possible to protect your device against malicious threat actors who would take advantage of system vulnerabilities. Attackers may target vulnerabilities for months or even years after updates are available.

Some software offers the option to automatically check for updates. If automatic options are available, it is recommended that you take advantage of them. If they are not available, periodically check your vendor's websites for updates.

Be sure to only download software updates from trusted vendor websites. Do not trust a link in an email message, attackers have used email messages to direct users to websites hosting malicious files disguised as legitimate updates. Users should also be suspicious of email messages that claim to have a software update file attached, these attachments may contain malware.

What is end-of-life software?

"End-of-life" or EOL is a term used by software vendors indicating that it is ending or limiting its support on the product and/or version to shift focus on their newer products and/or version. Continued use of EOL software poses a great risk to your system that can allow an attacker to exploit security vulnerabilities. The use of unsupported software can also cause software compatibility issues as well as lower levels of system performance and productivity.

The Guyana National CIRT recommends that users and administrators stop the use of all EOL products.

Best Practices for Software Updates

Enable automatic software updates whenever possible. This will ensure that software updates are installed as quickly as possible.

Do not use unsupported EOL software.

Always visit vendor sites directly rather than clicking on advertisements or email links.

Avoid software updates while using untrusted networks.

New vulnerabilities are continually emerging, but the best defense against attackers exploiting patched vulnerabilities is simple: keep your software up to date. This is the most effective measure you can take to protect your devices.

References

- Understanding Software Patches and Updates (19th November, 2019). Retrieved from US-Cert: https://us-cert.cisa.gov/ncas/tips/ST04-006

Software Updates and Patches (11th February, 2021). Retrieved from Kinetix: https://www.kinetix.com/blog/what-is-a-software-patch