# Keeping applications and operating systems up to date

## Introduction

Known weaknesses in outdated software can be exploited by hackers, creating serious cybersecurity issues. In this reading, you will explore various methods of updating Windows, Linux, and macOS operating systems. You will also dive into some recent historical incidents that illustrate the risks of not updating software.

However, before jumping into updating applications, let's start with an exploration of zero-day vulnerabilities.

## What is a zero-day vulnerability?

Zero-day vulnerability refers to a software security flaw unknown to those who should be interested in its mitigation (including the software vendor). As the vendor has had zero days to patch it, these vulnerabilities can cause extensive damage. These threats are often used in targeted attacks, where cybercriminals aim to compromise specific organizations or individuals. Even with the best security measures in place, organizations can fall victim to zero-day attacks.

### Mitigating zero-day vulnerabilities

Businesses can use threat intelligence services and sophisticated security solutions to spot unusual behavior to combat zero-day attacks. For example, artificial intelligence (AI) and machine learning (ML) technologies can help identify potential zero-day attacks based on unusual behavior rather than relying on known signatures of malware. Promptly installing updates once they become available is also critical to minimizing the window of opportunity for potential attackers. Disabling or uninstalling the application can also help until a patch is released.

It's also crucial to implement a robust incident response plan. This plan should outline the steps to take in the event of a security breach, including identifying and isolating affected systems, investigating the incident, and restoring services. Regularly testing and updating the incident response plan ensures that it remains effective.

## The consequences of not updating software

Historical incidents demonstrate the significant risks associated with not updating software. As you discovered earlier, the 2017 WannaCry ransomware attack exploited a known vulnerability in outdated versions of Microsoft Windows, causing havoc worldwide. Similarly, the 2014 Heartbleed bug affected servers running an outdated version of OpenSSL, leading to a massive security breach where hackers could access user passwords and other sensitive data.

But how can you keep your applications and the operating system up to date? Let's find out.

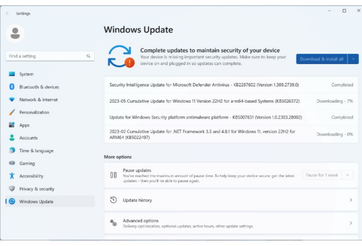
## Updates on Windows

Windows Update, which is a built-in tool on the Windows operating systems is used for updating your system and several key applications. This tool checks Microsoft's servers for new updates and automatically installs them on your computer.

To manually check for updates:

1. Open **Settings**.
2. Select **Update & Security**.
3. Select **Windows Update**.
4. Choose **Check for updates**.

If there are updates available, they'll be downloaded and installed.




For other installed applications, most have built-in update checkers that will notify you when a new version is available. If not, you may need to visit the application's website or distribution platform to download and install the latest version.

## How updates work in Windows

The Windows Update Orchestrator on your PC checks the Microsoft Update server or your WSUS endpoint for new updates at random intervals. The randomization ensures that the Windows Update server isn't overloaded with requests all at the same time. The Update Orchestrator searches only for updates that have been added since the last time updates were searched, allowing it to find updates quickly and efficiently.

When checking for updates, the Windows Update Orchestrator evaluates whether the update is appropriate for your device. It uses guidelines defined by the publisher of the update, for example, Microsoft Office including enterprise group policies.

Once the Windows Update Orchestrator determines which updates apply to your computer, it begins downloading the updates if you have selected the option to automatically download updates. The update is completed in the background without interrupting your normal use of the device.

To ensure that your other downloads aren't affected or slowed down because updates are downloading, Windows Update uses "delivery optimization", which downloads updates and reduces bandwidth consumption.

In the majority of cases when the option to automatically install updates is configured, the Windows Update Orchestrator automatically restarts the device for you after installing the updates. It has to restart the device because it might be unsecured or not fully updated until the restart takes place.

## Updates on macOS

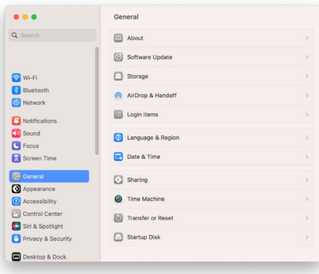
On a Mac, system updates and updates for apps downloaded from the App Store can be found in the same place:

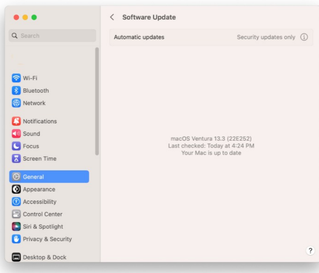
1. Open the App Store.
2. Select the **Updates** tab.
3. If updates are available, there will be a notification, and you can click **Update All** to install all available updates.

For apps not downloaded from the App Store, the process can vary. Some have a built-in updater or notify you when a new version is available. Otherwise, you will need to visit the app's official website to download and install the latest version.

On a Mac running the latest operating system:

1. Go to **System Preferences.**
2. Select **General.**
3. Select **Software Update** to check if there is any update available for the core operating system.
4. From here, you can also set the automatic update policies as per your requirement.




## Updates on Linux

Each Linux distribution has its own package management system for software updates. However, most of them can be updated using commands in the terminal. You have to check the manual or documentation of your current distribution to find out the best update policy available for that particular distribution.

In Ubuntu and other Debian-based distributions, you can update all your software by opening a terminal and typing the following commands:

1. `sudo apt update`
2. `sudo apt upgrade`

The first command updates the list of packages and their versions, and the second installs the updates.

In Fedora, CentOS, and other RHEL-based distributions, you can update all your software using the following commands:

- `sudo dnf check-update`
- `sudo dnf upgrade`

Again, the first command checks for available updates and the second command installs them.

## Conclusion

You explored various methods of updating Windows, Linux, and macOS operating systems in this reading. You also discovered how to use the built-in software update tools and gained an understanding of zero-day vulnerabilities before examining several real-world incidents that have occurred in the recent past.

Updating software may be a simple task, but it's vital for keeping your computer safe. This involves knowing how to update different operating systems, staying alert to new types of cyber threats like zero-day vulnerabilities, and ensuring everyone in your organization understands the importance of cybersecurity. By regularly updating your software and following good security practices, you can prevent many possible cyberattacks.

Mark as completed