

Introduction

A patch is a fix to software which is designed to improve its performance and/or address security vulnerabilities. A vulnerability is a "chink in the armour" of software, exposing a weakness which can be exploited, making patching a critical process for businesses to follow.

Why is patching important?

By not applying a patch, you might be leaving the door open for malicious software (malware) to compromise your systems. Malware often exploits flaws in a system to do its work. Unpatched defects in software may allow cybercriminals to infect or compromise your device with no action on your part.

What are hackers interested in when they exploit flaws on your computer?

When flaws are located and exploited, they can give hackers just enough time to download ransomware software (as an example).

Hackers are then able to encrypt all your files, making them unreadable while demanding a ransom to regain access. This information can include your client information which can be used to make your customers targets as well.

Detecting vulnerabilities and weaknesses in software

- ☐ Check your server, applications and operating system (e.g. iOS, Windows) provider's official website for updates.
- ☐ Vulnerabilities may present as a reduction in system performance, an incomplete security check or incompatibility with other networks and applications. These vulnerabilities make you susceptible to hackers looking for an easy way in.
- ☐ Subscribe to the [ACSC's Alert Service](#) to keep up to date on vulnerabilities and how cybercriminals are targeting Australian businesses.

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.

Preventing compromises

- ☐ New vulnerabilities in operating systems or other software are always being discovered and exploited, so it is always important to keep your software up to date.
- ☐ [Turn on automatic patching software](#) for Windows.
- ☐ [Turn on automatic patching software](#) for MacOS.
- ☐ Alternatively, you can access the individual software program you want to patch and follow the prompts to update the software.
- ☐ Use a reputable antivirus to detect and remove malware.

For additional support or information, contact IDCARE:

Submit [Get Help Form](#) | 1800 595 170 (Aus) | 0800 121 068 (NZ)

Sharing & Disclaimer

IDCARE is a not-for-profit and registered Australian charity.

© Copyright Identity Care Australia & New Zealand Ltd. While every effort has been made to ensure the accuracy of the information in this document, IDCARE disclaims any liability to any person with respect to any actions performed or not performed as a result of the contents of this document.