Information Security Essentials

Application Patching

THIS PAGE INTENTIONALLY LEFT BLANK

Application patching refers to applying updates to software applications. It is absolutely critical for ensuring system security and must be done as soon as practicable. Time is key with patching: it is ideal to apply patches within 48 hours of release from the relevant software provider or vendor. When installing new applications, always use the latest version which typically includes the latest patches. For some vendor applications, upgrading to the latest version is the only way to patch a security vulnerability and in most cases, this is the preferred approach to managing the ongoing task of patching your applications.

Note: To maintain visibility of what software requires patching, keep a consistently up-to-date inventory of software installed on every computer, especially devices that might only occasionally connect to the organisation's network such as spare or older machines, field laptops and handheld data capture devices.

In the SECMON1 blog post 'Security Overview - Information Security Essentials', we spoke about what application patching is and why it is an essential security measure.

In this document, we are going to provide some basic application patching steps for the most consistently vulnerable applications (Microsoft, Adobe and, web browsers), as well as provide you with some interesting and important links where you can educate yourself further on this topic and identify what other options are available to you.

There are some vendor-provided application patch management solutions available. Below are a few to give you a starting point to understand what solutions are available to you. We do not advocate or recommend any particular solution and would encourage you to take further steps to identify other solutions available.

- Cloud Management Suite
- Kaseya VSA
- SolarWinds Patch Manager
- Ivanti
- Automox

Implementation Guidance

When performing patching, organisations may be concerned about the risk of a patch breaking systems or applications, including any subsequent outage this may cause. While this is a legitimate concern, and should be considered when deciding what actions to take in response to security vulnerabilities, many vendors perform thorough testing of all patches prior to their release to the public. Often the immediate protection afforded by patching an extreme risk security vulnerability far outweighs the impact of the unlikely occurrence of having to roll back a patch (the process of restoring the application back to its original state prior to the patch being applied).

The following are the recommended deployment timeframes for patches based on the outcome of risk assessments for security vulnerabilities:

Extreme Risk: Within 48 hours of a patch being released

High Risk: Within 2 weeks of a patch being released

Moderate-Low Risk: Within 1 month of a patch being released

In situations where resources are limited, organisations are encouraged to prioritise the deployment of patches. For example, patches could be applied to workstations of high risk users (eg, workstations used by executive officers and their support staff, HR staff, FOI staff and public relations staff) within 48 hours, followed by all other workstations within 2 weeks.

Note: Some patching may require you to restart your computer. Most system restarts after patches can be deferred for up to 3 days.

It is advised to restart your computer at least once per week to allow patches to complete installations.

Further information

Further guidance, including applicability for non-Windows operating systems, is available at ASD Strategies to Mitigate Cyber Security Incidents.

How-To Guide

Software/Application Product Updates

Software/application updates are a bit easier to install than operating system updates. Some examples of software/applications on a business system are:

- Adobe products (eg, Acrobat, Air, Flash Player, and Reader)
- Browsers (eg, Chrome, Firefox, Internet Explorer, and Safari)
- Java
- Microsoft Office

A lot of software/applications will automatically check for and install updates. They will sometimes even display a pop-up when opening the software/application that there is a new version available.

To check if a software/application is up to date:

1. Open the software/application

2. Navigate to the **Help** menu and select **About**
3. Information about the current version will be displayed as well as a button for checking updates. Click the **Check for Updates** (or even just **Updates** in some software) button. This will allow the software/application to install the most current update or version.

Final Note

We at SECMON1 are available to review your application patching strategies with you and advise on troubleshooting as well as potential improvements and solutions. We are also available to implement application patching for your company.

Please feel free to visit our website at www.secmon1.com.

You can also reach us by phone at 1300 410 900 or by e-mail at contact@secmon1.com.