



## What You Need to Know about Patch Management

### *Patch Management*

Patches are issued regularly by most software vendors, some as often as once a month. The most common types include:

- **Fixes for Security Concerns** - Resolution for newly discovered vulnerabilities
- **Bug Fixes** - Corrections for things that aren't working properly
- **Feature Updates** - Additions of new features or improved stability
- **Compatibility Updates** - If the software in question is a driver, there may be patches to offer compatibility with additional hardware

### *What is the Danger of Not Handling Patch Management*

The biggest danger of not keeping up with your organization's patch management is the potential security risk. Your systems can become vulnerable to hacker attacks, network breaches, and viruses. Your company can be brought to its knees by a completely avoidable problem.

If your organization either contracts with a government or security agency or is a government or security agency, not installing security patches in a timely manner can cause you to become out of compliance with your contract or mandate. In addition, if you install a patch without testing it first, the "law of unintended consequences" says that all manner of things can go wrong.

### *What is the Recommended Patch Management Process?*

The best way to handle patch management is to automate as much of it as possible through your network monitoring system. Coyote Creek handles patch management for many of our clients. Here is the 7-step process that we follow:

1. **Discover Available Patches.** This is best done through patch management software.
2. **Determine Patch Priority.** In general, the patch's priority level is initially determined by the vendor. Microsoft, for example, will attach a "high priority" or "highly critical" label to patches that they deem to be most important, especially those relating to security vulnerabilities. However, even patches that are not labeled as "high priority" by the manufacturer can be extremely critical for you.
3. **Create a Back-Up Plan.** Just because a patch is deployed by a reputable vendor doesn't mean it won't adversely affect your machine when you load it! What will you do if things go wrong? How will you get your server back to the state it was in before the patch was installed?

In order to create a workable back-up plan you must have a thorough understanding of what the patch does. Typically you will simply plan to uninstall the patch. However, this isn't always possible. Certain patches for Microsoft Exchange, for example, make changes to the overall infrastructure of the application that cannot be undone once the patch has been installed.

4. **Test the Patch.** To avoid potential problems it is best to start by installing the patch in a testing infrastructure that will have minimal impact on your production. Wait three to four business days after installation, to see if any problems turn up. Ideally you should run a load simulator against the server, to confirm that the test server responds normally under a load. If all goes well, deploy the patch in stages to your environment, starting with the most non-critical servers.

Coyote Creek's policy is to deploy all patches in stages, always waiting at least three to four business days in between stages. This eliminates down time and avoids problems. Not all companies take the time to do this, but we believe it's critical for safeguarding our clients' systems.

5. **Monitor the Patch.** After a patch has been installed, problems can be obvious or they can be subtle. The key is to carefully monitor your system at each stage of patch deployment, starting with the first test.

Compare your post-installation stats to your pre-installation baseline. Have any unexpected changes taken place? Is your monitoring system telling you that something is awry?

6. **Deploy the Patch.** If you have one or two machines, deployment is a simple process. But if you have hundreds or thousands of machines you'll either need a deployment application or a lot of people working nights and weekends to get the job done. Coyote Creek can help you determine the best deployment solution for your environment.
7. **Make Use of Patch Reports.** Most network monitoring tools can be configured to provide reports on which patches have been deployed and which are missing, for each of your organization's servers. This information can be beneficial for everyone involved with managing the IT function within your organization.

#### *How Can Coyote Creek Help?*

Coyote Creek Consulting has been offering network monitoring services – including complete patch management – for over seven years. We've handled patch management for thousands of servers in a wide variety of infrastructure environments. We know what to look for, how to determine a patch's priority for your organization's specific needs, and how to deploy patches in such a way that disruptions are kept to a minimum. Our experience supporting the unique needs of a multitude of companies gives us a good understanding of the importance of and potential issues surrounding particular patches out in the field.

Many organizations find that handling network monitoring and patch management is not the best use of their employees' time. Coyote Creek offers these services either on site or remotely, and can get things set up in less than 2 weeks. If you have any questions about patch management or network monitoring just give us a call. We're here for you.