Reference <https://www.itpro.co.uk/security/27713/the-importance-and-benefits-of-effective-patch-management>

**Patch management vs vulnerability management**

**What exactly is patch management, and why should IT pros sit up and take notice of doing it properly?**

by: [Keumars Afifi-Sabet](https://www.itpro.co.uk/authors/keumars-afifi-sabet)

27 Jan 2021



When it comes to developing software, the work never stops. Code and  capabilities change and evolve so much that no system can be left  untouched, no matter how well it is built, and monitoring and deploying  security patches is a never-ending source of work for [IT teams](http://www.itpro.co.uk/security/34257/it-pro-panel-why-is-patch-management-so-difficult).

If you think of the IT equipment with an organisation - [laptops](https://www.itpro.co.uk/laptops/23742/Best-Laptops), [printers](https://www.itpro.co.uk/printers/29013/best-printers), [servers](https://www.itpro.co.uk/server-storage/30338/four-steps-to-a-successful-server-setup), and even mobile phones -  there are a multitude of entry points for any hacker. Being proactive and updating the software is a frustrating part of modern life, but it is an absolute must for organisations.

* [The cyber security skills your business needs](https://www.itpro.co.uk/security/28196/the-cybersecurity-skills-your-business-needs)
* [Four strategies organisations are using to combat cyber attacks](https://www.itpro.co.uk/endpoint-security/30837/four-strategies-organisations-are-using-to-combat-cyber-attacks)
* [Who should take ownership of your cyber security strategy?](https://www.itpro.co.uk/enterprise-security/34017/who-should-take-ownership-of-your-cyber-security-strategy)

Applying fixes and updates for security vulnerabilities is known as patch  management or 'vulnerability management'. The latter isn't as well known but is often used in tandem with the former, despite both having key  differences.

Essentially, vulnerability management is the process of dealing with [security vulnerabilities](https://www.itpro.co.uk/vulnerability/34184/what-s-the-difference-between-a-security-vulnerability-and-a-security-threat) of all guises. It is divided into four main stages: discovery, reporting,  prioritisation and response. And patch management is focused on the  application of software updates to address specific security flaws. It  can be part of a vulnerability management strategy, but the subject of  vulnerability management is actually much broader.

Top of Form

Bottom of Form

With [cyber attacks](https://www.itpro.co.uk/security/cyber-security/356354/uk-businesses-spent-ps87-billion-in-five-years-tackling-cyber-crime) on the rise during the pandemic, organisations have a constant battle on  their hands. The more online their business becomes, the more open they  are to attacks. As such, knowing the difference between vulnerability  management and patch management is crucial.

**What is patch management?**

Perhaps it's important to go back to basics for a moment. Patch management is  the process of making sure that every piece of software used within a  company is up-to-date with the most current versions (you might think  the version you've bought is the latest but bugs are routinely found  after GA and rather than just ignoring, vendors have to add a sticking  plaster until the next update) released by the manufacturer. This  includes enterprise-level products like server operating systems and  database products, as well as more basic tools like Internet Explorer  and Adobe Flash.

Patch management can be done manually on a machine-by-machine basis, but it's much more commonly performed using centralised management tools. This  can involve dedicated patch management software, which allows IT teams  to set policy-based rules for the automatic application of patches.  These can be scheduled around business hours to ensure that patch  application results in minimal downtime and loss of productivity.

**Why is patch management important?**

Unpatched systems are one of the easiest attack vectors for criminals looking to  gain access to corporate networks. Hackers and security researchers are [constantly discovering new vulnerabilities](https://www.itpro.co.uk/security/34097/exploits-for-windows-bluekeep-vulnerability-commercially-available), and companies are constantly issuing patches to deal with them. If  those patches are not applied, however, cyber criminals have an easy  entry point into your networks.

Patch management also ensures that all your enterprise equipment keeps working as it should. Technology is a notoriously fickle beast, and even minor software bugs can lead to  major headaches and plummetting employee productivity. Timely  application of patches ensures that any potential problems can be  resolved as soon as possible before your business grinds to a halt.

Knowing when not to apply an update can be just as important for good patch  management, however. New software updates can cause compatibility issues between different systems or [can introduce new bugs of their own](https://www.itpro.co.uk/microsoft-windows/34391/microsoft-breaks-even-more-windows-10-features-with-latest-patch). Good patch management often involved making a judgement call on whether or not the security benefits of installing a patch which is known to  cause issues are worth risking a little potential disruption.



**What is vulnerability management?**

Vulnerability management is a set of processes designed to secure corporate networks, divided into discovery, reporting, prioritisation and responses phases  with regards to pitfalls – each following sequentially one after the  other.

**Discovery**

The first phase, discovery, involves assessing all assets across the  breadth of your IT infrastructure, including servers, laptops, printers, screens, and backup appliances. Essentially all devices that may be  connected to a corporate network count, as well as software that’s  running. The discovery process must ascertain whether the developer  still supports the software with security patches, and how up-to-date  the software is.

This process may be arduous and lengthy, but  putting in the hard work at this stage is crucial. It’s essential to  ascertain a complete picture of the systems the business relies on, with unpatched hardware introducing needless gaps into the setup. This lack  of oversight was essentially the reason why [Equifax suffered in the infamous cyber attack of 2017](https://www.itpro.co.uk/security/34372/equifax-named-the-most-googled-data-breach-of-all-time). There are a host of network monitoring tools at disposal, thankfully,  that can lighten the burden slightly by detecting and querying network  devices.

**Reporting**

The reporting phase  follows on once you’ve established a full and up-to-date understanding  of the IT estate, and what hardware devices and software is connected to the corporate network. This information should be compiled into a  report that can be easy-to-read, accessible and referencable, detailing  the systems that are most vulnerable. This assessment would be based on  various criteria such as the severity of unpatched flaws, and how close  the systems and applications are to sensitive data.

It's possible to do this automatically using software, with many security  platforms allowing you to create reports and 'digests' based on the  results of autonomous network scans. Reporting feeds into the next step, prioritisation, and some vulnerability management programs class them  as part of the same stage.

**Prioritisation**

Arguably the most important stage of the vulnerability management process,  prioritisation is where you decide the order in which you're going to  address the vulnerabilities within your network. This will be based on a number of factors, but the principal things to consider are: how long  it will take to fix, how much it will cost to fix and how much risk it  poses. Which factor you give the most priority to will likely depend on  the individual circumstances of your business, but it's a good idea to  prioritise high impact, low-effort fixes where possible.

In many  cases, the likelihood of a flaw being exploited, or the potential impact if it is, will be low enough that you can judge leaving it unpatched to be an acceptable risk. Alternatively, the cost of fixing something may  be so high as to make it unfeasible with your current resources. The  important thing is to be able to identify these acceptable risks and to  be aware of them going forward.

**Response**

Having established what vulnerabilities your network has and what order you're going to address them in, the final stage is to respond to them. In  some cases, this can be as simple as installing any outstanding  infrastructure patches or reconfiguring a vulnerable network device.  Other measures may be more costly or time-consuming, however, such as  creating a patch for your own application or replacing a device that is  no longer supported by the manufacturer.

You can also take the  decision to mitigate an issue by partly addressing the problems or, as  mentioned above, by accepting the risks posed by a particular  vulnerability. Once you've completed the response cycle, the process  starts again with a fresh round of discovery to see what the state of  your network is after your actions to secure it.

**Why is vulnerability management important?**

Vulnerability management is crucial because it gives you an overview of your security posture as a whole. It gives you a sense of which areas of your  infrastructure are most at risk, which allows you to not only prioritise security remediation but also helps inform future IT investment.

More importantly, vulnerability management gives you insights into potential security holes beyond what you can learn from looking at a list of  outstanding patches. There may be a piece of software that is known to  be vulnerable, for example, but for which a patch is not yet available.  In this case, looking at unapplied patches would not have alerted you to the issue.