Reference <https://blog.rsisecurity.com/vulnerability-scanning-vs-patch-management-whats-the-difference/>

**Vulnerability Scanning vs. Patch Management: What’s the Difference?**

written by [RSI Security](https://blog.rsisecurity.com/author/rsi-security/)September 11, 2019

[](https://blog.rsisecurity.com/wp-content/uploads/2019/10/patch-management-vulnerability-scanning-woman.jpg)

In September 2017, Equifax, a  consumer credit reporting agency, has suffered a major data breach that  exposed the personal data of 148 million American consumers. This data  breach is related to the “critical vulnerability” in the Apache Struts  software that was publicly disclosed in March 2017. According to a[report](https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf) by the U.S. House Committee on Oversight and Reform released in  December of 2018, “Equifax used Apache Struts to run certain  applications on legacy operating systems. The following day, the  Department of Homeland Security alerted Equifax to this critical  vulnerability.”

On March 9, the Global [Threat and Vulnerability Management](https://www.rsisecurity.com/threat-vulnerability-management/) team of Equifax sent this alert via email to more than 400 individuals. They told anyone who had Apache Struts to apply the necessary patch  within 48 hours.

Equifax, however, didn’t apply the  necessary patch. This led to the exposure of their system and data for  76 days. The report implies the need for any business to reinforce,  emphasize and enhance the vulnerability scanning and patch management processes and procedures.

Vulnerability scanning and [patch management](https://blog.rsisecurity.com/patch-management-best-practices/)are two terms that are seemingly identical, but that is not the case. While they have a compatible relationship, they are not the same. It is  important for a business to learn the difference between these terms or  else it could suffer from a [cybersecurity attack](https://blog.rsisecurity.com/infographic-how-prepared-is-your-business-to-face-cyber-threats/) similar to that of Equifax.

Let’s define these two terms and see the difference.

**What is vulnerability scanning?**

Vulnerability scanning identifies and forms an inventory of all systems connected to a network. This includes printers, switches, [firewalls](https://blog.rsisecurity.com/firewall-essentials/), containers, virtual machines, laptops, desktops, and servers. For each  identified device, it also attempts to recognize the software installed  on it and the operating system it runs. This also includes other aspects such as user accounts and open ports.

Furthermore, it is a security method  used to detect and identify weaknesses in the IT systems. A scan may be  done by a business’ IT team or a security service provider as a  condition instructed by an authority.

It is the first part of the [vulnerability management](https://blog.rsisecurity.com/how-to-build-an-effective-vulnerability-management-program/)process which is the identification of vulnerabilities. The main way to  identify weaknesses in a system is through vulnerability scanning. The  scanner’s efficiency depends on two things: the scanner’s ability to  identify open ports, software, and devices and collect other system  information, and the scanner’s ability to associate this data with  identified information from one or more vulnerability databases.   Scanning can be built to be more or less invasive or aggressive. This  configuration is essential because there is a probability that the  scanning can have an effect on the performance of the system being  examined.

[Get a Free Vulnerability Assessment](https://www.rsisecurity.com/marketing/vulnerability-assessment/)

**Types of Vulnerability Scanning**

There are types of vulnerability  scanning and it is necessary to carry them out to make sure that a  business complies with certain standards and regulations such as [PCI DSS](https://www.rsisecurity.com/compliance-advisory-services/pci/) or the Payment Card Industry Data Security Standard. These types of vulnerability scanning are as follows:

* **Internal vulnerability scan. This scanning is carried out from inside a business’s firewalls or perimeter defenses and used to identify potential vulnerabilities internally. The purpose of this scan is to detect weaknesses that could be potentially  exploited by cybercriminals who penetrate the insides of a business’  network successfully.**
* [**External vulnerability scan**](https://www.rsisecurity.com/marketing/vulnerability-assessment/)**. In contrast, this scanning searches for vulnerabilities or holes carried out from outside a**[**business network**](https://blog.rsisecurity.com/network-security-best-practices-a-complete-checklist/)**where anomalous outsiders can invade and attack. These vulnerabilities  can be on the specialized web application firewall or on the open ports  inside the network firewall.**

These two types of vulnerability  scanning are performed in the same manner. Both are automatically run  through an Internet connection and a computer program. But there is no  program that can conduct both scans simultaneously.

It is critical to have both scans in  your business because hackers or malware aren’t just present outside a  business firewall, they can be on the inside of the network, too.



**Two Approaches to Vulnerability Scanning**

Additionally, these scans could be  performed through two approaches: authenticated and unauthenticated  scans. In the authenticated approach, the person doing the scan logs in  as a local network user. This leads to the revelation of vulnerabilities and other findings that are only available to a trusted user, or to a  malicious attacker that has invasive access to the network and gained  entry as a trusted user.  On the other hand, an unauthenticated scan  revolves around mimicking an intruder’s ways to scan the network,  without trusted access to the system. The unauthenticated method reveals findings and vulnerabilities that are accessible to outside users or  are available even without logging into the network.

Ideally, any detected vulnerabilities after a [vulnerability scanning](https://blog.rsisecurity.com/what-to-expect-when-going-through-an-external-vulnerability-scan/) is performed should be patched in order that they no longer identify  vulnerabilities that pose a threat. This is where patch management comes in.

**What is patch management?**

[Patch management](https://blog.rsisecurity.com/what-is-the-patch-management-process-for-nerc-cip/) is the process of managing a business’ network of computers by  installing and applying, in a timely manner, all missing patches to  ensure that these computers are up to date. Furthermore, it is the  process of managing all updates of machines and devices within a  business information system. These devices and machines include  anti-viruses, operating systems, servers, firewalls, routers, among  others.

Software companies mostly perform  patch management as part of their efforts to fix issues within their  network. It is also done to features.

Common and popular examples of patch management are Windows, Mac, and Linus patch management.

[Assess your Patch Management program](https://www.rsisecurity.com/patch-availability-report/)

**Automating Patch Management**

It is very important to automate  patch management because manually monitoring and updating a business’  network of computers could possibly cause loss of time intended for  other valuable security tasks. [Patch management](https://blog.rsisecurity.com/patch-management-wannacry/) software for your business can be automated to allow all the computers  in a network to be up to date with the current releases of patches.

There are things to consider in  having automated patch management. First is the security of a business’  network. To decrease the [threat](https://blog.rsisecurity.com/top-10-network-security-threats/) of having a security attack and other related issues, it is important  to do automation because a business should always look for the latest  bug fixes, security patches, and vulnerability protection.

Another thing to consider is [compliance](https://www.rsisecurity.com/compliance-advisory-services/). As instructed by certain regulators and authorities, all businesses  should be well-secured and able to protect their own data and the  information of their customers and partners. That’s why it’s important  to automate patch management to adapt to a rigorous vulnerability  strategy. If any business fails to comply, it could face legal and  financial problems or worse, loss of business.

Furthermore, it is important to  consider the productivity of a business. Because manual patching is  time-consuming and difficult to carry out, automated patch management is important to speed up the process and improve the stability of a [network’s security](https://blog.rsisecurity.com/network-security-best-practices-a-complete-checklist/).

**Reasons why you need patch management**

There are many reasons why patch management is important to be carried out by any business, these include the following:

1. It is one  of the most vital tasks of a business’ IT team because if an operating  system or software is left unpatched, a business could be at risk of  serious cyberattacks.
2. Cyber  attackers are ready and on-the-go to exploit unpatched networks right  after the release of a security update. That’s why updates and upgrades  should be performed in a business’ network of computers immediately.
3. [Patch management](https://www.rsisecurity.com/patch-availability-report/) is important because it’s not only difficult and time-consuming to  manually monitor and apply security updates, it’s also unsafe. Even a  little interruption in installing the updates could put a business’s  network at risk of vulnerabilities.
4. A  business’ patching software offers automated patching which allows the  IT department to attend to more important IT security tasks.



**Difference between vulnerability scanning and patch management**

Vulnerability scanning and patch management have a compatible relationship, but they are different in the following manner:

Vulnerability scanning is the first stage of vulnerability management. The [vulnerability management](https://blog.rsisecurity.com/vulnerability-management-from-an-mssp/)process includes 5 stages:

* **First stage.** Discovering vulnerabilities (this is where vulnerability scanning is  performed, where vulnerabilities are discovered and  identified)
* **Second stage.** Assessing vulnerabilities
* **Third stage**. Reporting vulnerabilities
* **Fourth stage.** Remediating vulnerabilities
* **Fifth stage.** Verifying vulnerabilities

On the other hand, patch management  is also a part of the vulnerability management process, but it is a  superset of vulnerability management and is included in this equation:

**Vulnerability Management = Policy + Awareness + Prioritization + Patch Management + Testing + Tweaking + Mitigation**

Vulnerability scanning is performed to [identify threats and vulnerabilities](https://www.rsisecurity.com/services/managed-detection-response/). When identification is done, the remediation path should be pursued and that’s where patching vulnerabilities come in. A business usually gets  patches from the vendors of the affected software or hardware.  All  vulnerabilities or the affected areas of the network should be patched  to remain up-to-date and safe from risks and attacks.

Vulnerability scanning and [patch management](https://www.rsisecurity.com/patch-availability-report/) are crucial to a business’ vulnerability management program. Knowing  the definition, importance of, and differences between these two  processes is as critical. These are all parts of [vulnerability management](https://blog.rsisecurity.com/what-are-the-different-managed-vulnerability-services-available/) and executing these methods appropriately will absolutely prevent a  business from vulnerabilities and potential cybersecurity threats and  damages.