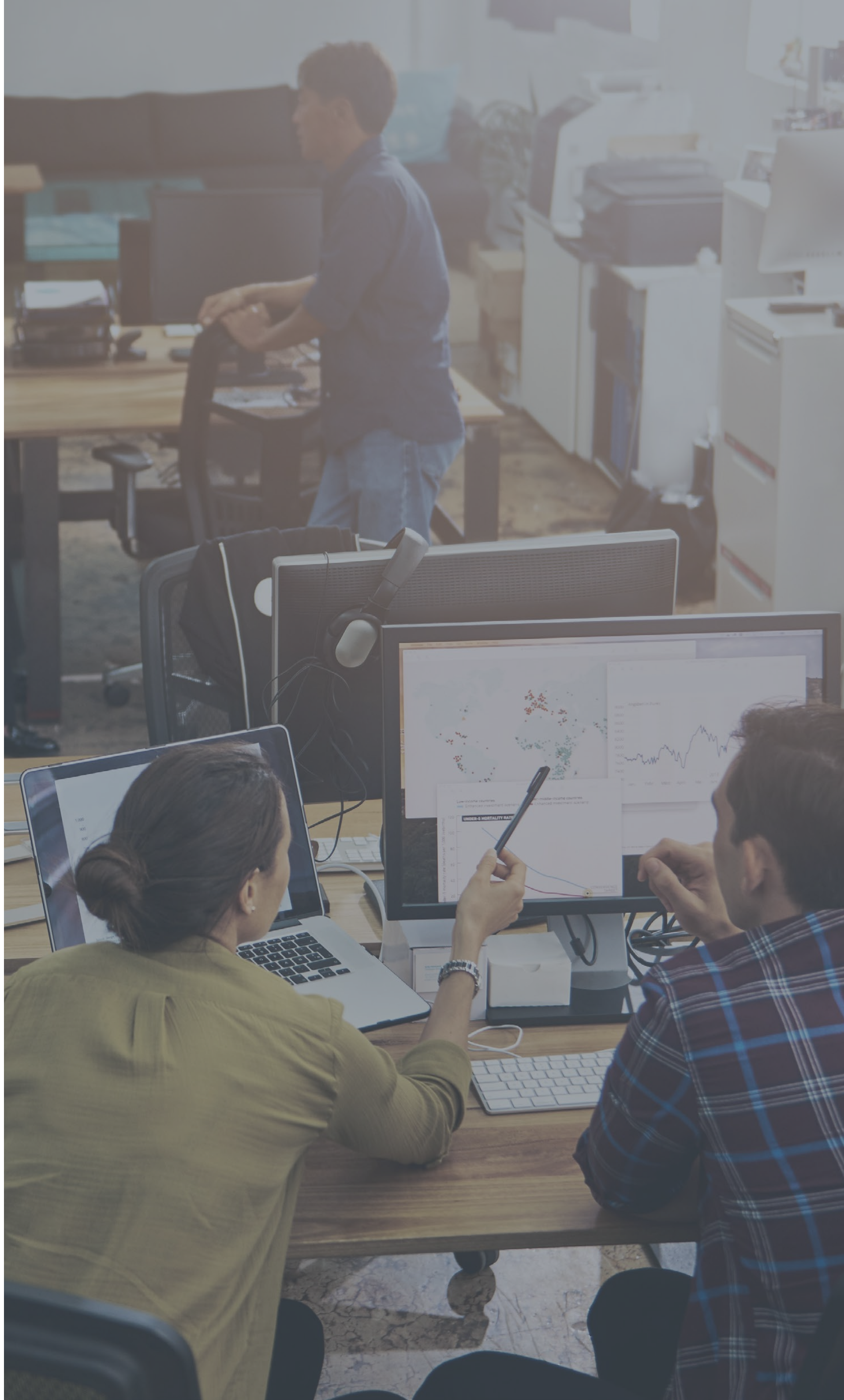
Patch Management:

Your Biggest Ally in the War Against Cybercrime

panda

pandasecurity.com

Table of Contents



Introduction

Would you believe that most of today's security incidents could be completely avoided?

It's true. The majority of attacks and exploits today take advantage of outdated systems and third-party applications, exploiting known vulnerabilities. Vulnerabilities for which patch updates have been available weeks, months, or even years before the breach. It's a trend that shows no signs of slowing down: Gartner predicts that by 2020, 99% of the vulnerabilities that cause security incidents will be known before an incident takes place, meaning a timely update would be enough to stop it from happening.

Although it's true that most incidents can be avoided by keeping systems updated, the reality is not always that simple. Many organizations struggle to keep their networks up to date due to a variety of factors, including digital transformation, an increased number of vulnerable endpoints, network complexity, decentralized management and more.

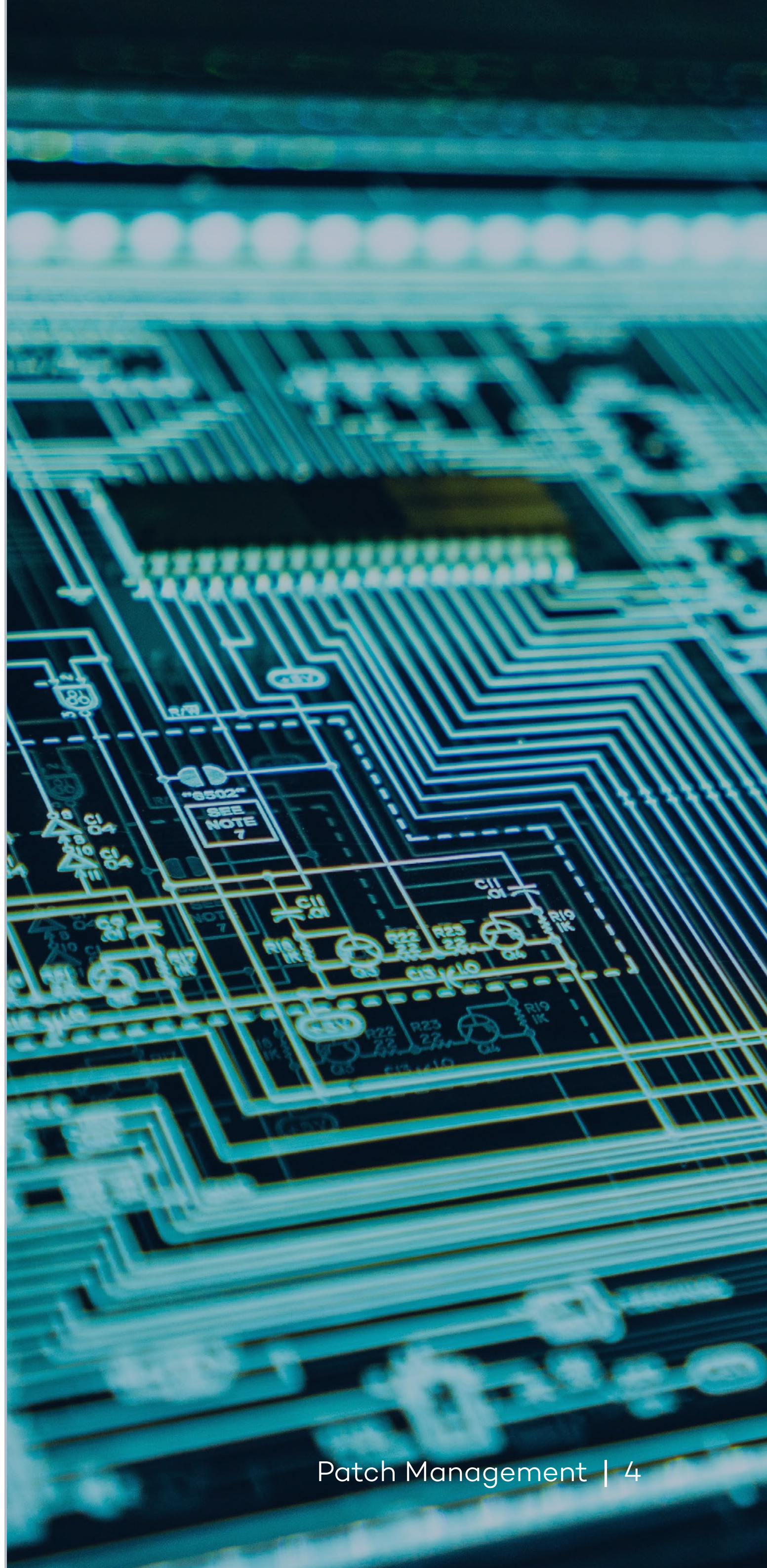
It's no longer a question of if, it's a question of when your organization is going to be the victim of a breach. Are you prepared to detect and respond before serious damage is done to your business? This eBook will walk you through the dangers of vulnerabilities, including the new BlueKeep vulnerability, and ways you can keep your organization safe.

The Danger of Vulnerabilities

The list of cyberattacks enabled by vulnerabilities is long, and it's growing. The most notorious attack in recent memory, WannaCry, was made possible thanks to a Windows vulnerability called EternalBlue. And earlier this year, the discovery of BlueKeep, a vulnerability in Windows XP, 7 and other Windows systems, was announced. BlueKeep exists in Remote Desktop Services, and like EternalBlue, is potentially wormable, meaning it could be used to launch a piece of malware that self-propagates between systems containing the same vulnerability. The similarities between EternalBlue and BlueKeep are troubling to cybersecurity professionals because it means that, in theory, BlueKeep could be used in a cyberattack similar in scale and impact to WannaCry.

Even with patches readily available, these vulnerabilities are still being used to carry out large scale cyberattacks. Almost two months before the WannaCry attacks, Microsoft had published a patch to fix EternalBlue, and computers that had installed it were not affected. More recently, many experts believe EternalBlue was behind a major attack on the City of Baltimore in 2019, two full years after the patch was issued. The ransomware attack took out large parts of the city hall's IT systems, and over three weeks later, the city is still trying to recover its systems.

Both these cases could have been completely avoided by employing proper patch management practices. These examples are startling proof that illustrates both how important security updates are, as well as how many organizations lack the time and resources needed to monitor vulnerabilities and patch updates.



Possible Cybercrime Activity

Because of the potential for a large-scale attack, the IT security community has been monitoring the BlueKeep vulnerability for signs of attacks or PoC (proof of concept) demos that could be used to exploit the vulnerability. Although there has not yet been an attack carried out by exploiting BlueKeep, threat actors have been detected scanning the Internet for systems containing the BlueKeep vulnerability.

On May 24, 2019, threat intelligence company, GreyNoise, announced that it had started to detect scans that were looking for Windows systems with the BlueKeep vulnerability. It is believed that this activity is being produced by a single cyberattacker.

For now, these are just scans, and no attempt has been made to exploit the vulnerability. However, the fact that an attacker is dedicating time and resources to compiling lists of vulnerable devices suggests that it is likely that an attack is being prepared. And with an estimated total of one million vulnerable devices, this attack could have devastating consequences.

While no researchers have published any exploits for this vulnerability, several organizations have confirmed that they have successfully developed BlueKeep exploits, which they will keep private to avoid facilitating their use in cyberattacks. At least six organizations have developed exploits for BlueKeep, and there are at least two very detailed reports about the vulnerability. The more testing is done to understand BlueKeep, and the more information starts floating around, the more likely that information is to land in the hands of cyberattackers. When that happens, it is only a matter of time before they launch a full-scale attack.

Staying Protected

Although no attacks have exploited it yet, it is vital to close the BlueKeep vulnerability, given the likelihood of it being used in a real attack. When the vulnerability was discovered, Microsoft launched a patch for the affected systems, including Windows XP, Windows 7 and Windows Server 2008. This patch should be installed as soon as possible.

To protect against EternalBlue, BlueKeep or any cyberthreat, it is important to have an advanced cybersecurity solution in place. Panda Adaptive Defense provides complete visibility over endpoint activity on your network, so that you know exactly what is happening across your network at all times.

One of its modules is Panda Patch Management, which requires no additional deployment, and provides patches and updates for the operating system as well as hundreds of third party applications. Panda Patch Management audits, monitors, and prioritizes updates from a single panel. It is also able to remotely isolate computers from the network while you patch them. Panda Patch Management mitigates attacks that exploit vulnerabilities, applying a constant critical update policy to detect any possible threat, even before it becomes dangerous.

Benefits of Patch Management

Panda Security's vulnerability management solution presents numerous advantages:

Discover, plan, install, and monitor

Provides visibility of endpoint health in real time, in terms of vulnerabilities, patches or pending updates, and unsupported software (EoL).

Prevents incidents, systematically reducing the attack surface created by software vulnerabilities

The management of patches and updates with easy-to-use, real-time management tools that enable organizations to get ahead of vulnerability exploit attacks.

Reduces operating costs

No deployments or updates needed. No effort required as updates are launched remotely from the web console, and it provides immediate visibility of vulnerabilities, updates and EoL applications.

Audit, monitor, and prioritize updates on operating systems and applications

Updated in real time, it offers an aggregated visibility of the status of the patches and pending updates for the systems and hundreds of third party applications.

Contains and mitigates attacks, immediately patching one or several endpoints

The console correlates detected threats and exploits with the uncovered vulnerabilities. Response time is minimized, containing and remediating attacks by pushing out patches immediately from the web console.

Helps with compliance with the accountability principle

Many regulations, like HIPAA, PCI, CCPA or GDPR force organizations to take the appropriate measures to ensure protection of the sensitive data under their control. Panda Patch Management helps you to comply with this obligation.

More info at:
www.pandasecurity.com/usa/business

Let’s talk:

1-407-215-3020

sales@pandasecurity.com

pandasecurity.com