The Real Risk of Patching

Erik Johnson, Director Reliability Analysis

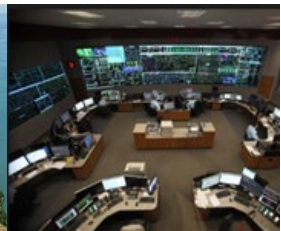
2021 Fall Reliability and Security Seminar

November 15, 2021

PUBLIC





The Tie to Configuration Management

- **Patch management within configuration management?**
  - Not purely a technical pursuit
  - Must be tied to the policies, processes, and procedures that support configuration management.
- **Programs can vary in approach but the goal should be:**
  - A consistently configured environment that is secure against known vulnerabilities in the operating system and application software.

Tying It All Together, With Eyes Up

- **The tie to configuration management for patching supports:**
  - Contingency and back out plans
  - Recovery plans if something goes wrong
  - Specific milestones and acceptance criteria
- **Further, the tie to configuration management should include vulnerabilities handled through:**
  - Applying a patch
  - Not applying a patch and using a mitigation plan
  - Zero-day vulnerabilities

Compliance Obligations vs Risk

You might be thinking: Zero-day vulnerabilities – I have enough to do, and besides there is no patch, so what does it matter?

Consider this:

- It's estimated that 80% of endpoint compromises are the result of Zero-day exploits. [1]
- 2021 has broken the record for zero-day hacking attacks. [2]

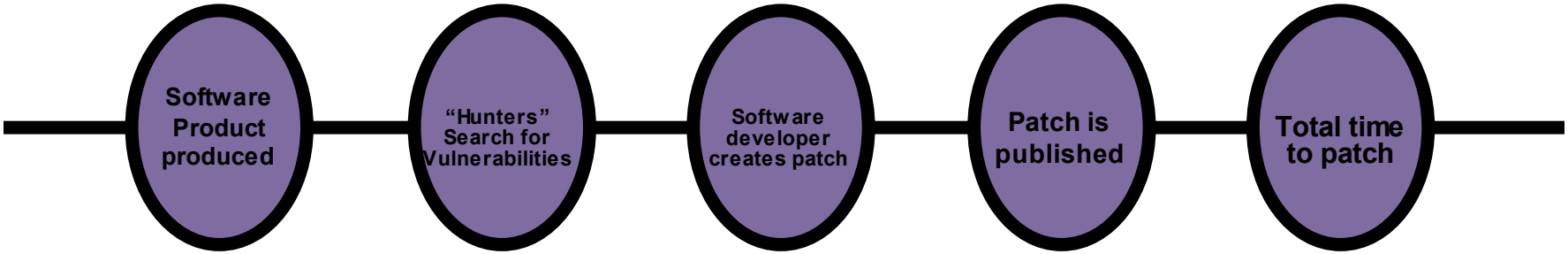
1 www.securityinfowatch.com/cybersecurity/press-release/21123576/ponemon-institute-ponemon-institute-reveals-68-of-organizations-were-victims-of-successful-endpoint-attacks-in-2019

2 https://www.technologyreview.com/2021/09/23/1036140/2021-record-zero-day-hacks-reasons/

Zero-Day

OK, but I have 35 days to evaluate a patch once it's available, so can I still be compliant?

- You can, but can you be secure, as well? Let's look at a simple example of how a Zero-day has an impact on that 35-day mark.



Initial Development Complete Product Available for Purchase

Vulnerability Found with two possible paths

Good path: "Hunter" will report

Bad path: "Hunter" sells or uses

Patch assigned a severity by vendor

CVE is assigned by a CVE Numbering Authority (CNA)

NERC CIP-007-6

R2 Part 2.2 35 day clock starts

Evaluation + total time of 2, 3 & 4

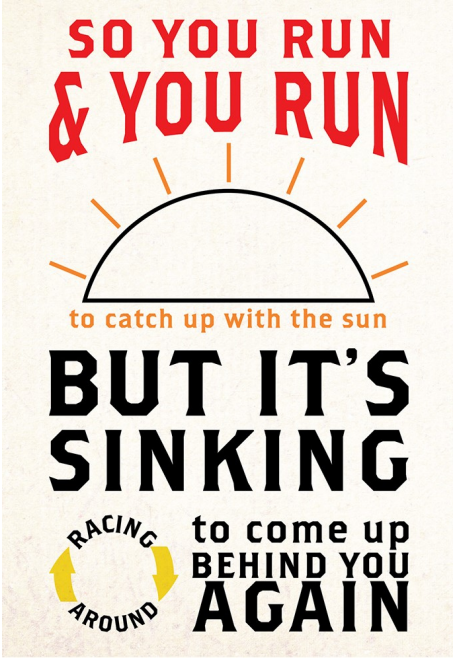
For discussion purposes :10 week days + 10 week days + 35 = 55 Days unpatched (best case)

Preparation is Key

- **Change and configuration management around security patching processes and practices can better protect your organization from Zero-day exploits.**
  - There are resources you can use to identify zero days, but they are still developing and only include the vulnerabilities identified by ethical individuals.

    Zero-day Initiative

- **74% of threats detected in Q1 2021 were zero day malware – or those for which a signature-based antivirus solution did not detect at the time of the malware release.**[1]



1 www.darkreading.com/vulnerabilities---threats/74--of-q1-malware-was-undetectable-via-signature-based-tools/d/d-id/1341394

Reality

- **The real approach should include:**
  - Researching Zero-days
  - Layers of security to harden the environment accordingly
  - Do you have examples?

- **There is very little data on reported recovery times, but the mean time to remediation (MTTR) is around 60 days. [1]**

1 www.comparitech.com/blog/information-security/cybersecurity-vulnerability-statistics/

Conclusion

- **Focusing on a "check-the-box" approach can keep you compliant, but there are other residual risks that need to be addressed.**
  - Any type of standard is put in place for a purpose, but their required processes make them too big to react to the changing landscape.
- **Onion Theory for information security**
  - Defensive layers that support each other
    - AKA defense in depth or the castle approach
- **Why is it always passive?**
  - Why not use the layered tools at our disposal, such as configuration management, in a more active manner to address the changing landscape?

Questions & Answers

Forward Together ReliabilityFirst