Avoiding Operational Nightmares by Adhering to Basic Security Guidelines

Sven GABRIEL, Tobias DUSSA

EOSC-hub receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 777536.

Introduction

- Some examples of typical “operational nightmares.”
- What went wrong.
- What the impact was.
- How to address the issue and mitigate the impact.

Operationally-Challenging Situations

- Widely used service not available when many users need to access it (Confluence incident).
- Housekeeping.
- Reaction time windows for patching.

Example 1 — Degraded Service Availability when Everyone is Watching

Confluence Incident

- Vulnerability in Confluence modules (CVE-2019-3396) abused.
- Multiple actors with interest in crypto-currency mining
- Incident detected on April 10.
- Earliest evidence of vulnerability exploitation: April 4.
- Confluence security advisory: 2019-03-20.
- **Service used for a conference April 9 through 12.** Responsibilities?

Example 2 — Housekeeping

Web-Based Crypto Miner

- Web-based crypto-mining JavaScript planted.
- Impact: Visitors' CPUs abused.
- Web server provided information about a finished project, not maintained any more

Example 3 — Popular Software Needs to be Patched ASAP

WordPress incident/what happened

Sep 03 13:45 - EGI CSIRT notified, about when visiting egi.eu under targeted conditions, an html-payload based redirect to several malware domains, forensics timeline:

- Auf 25 and 26 PoS for the vulnerability published
- Sep 1 A security fix was announced be Wordpress
- accesses seem to drop some shell/C&C that was used to access the machine later.

zero-day vulnerability (later marked CVE-2020-25213) allowing unauthorized remote user to execute arbitrary code on the server resulted in internet wide campaigns deploying malicious code used to control the data served to the web site visitors.

Become More Resilient — Basic Security Guidelines

Patching, Patching, Patching

- Keep your machines up-to-date.
- Install patches.
- Make sure updates are deployed.
- Apply security fixes.
- Do not forget to patch.

Patching — Operational Considerations

- Ideally: (Security) updates are installed automagically.
- However, this creates operational hazards: Downtime, potentially hard-to-troubleshoot issues, . . .
- Trade-off needs to be balanced.
- (If the update process is sufficiently broken, maybe the software should not be used in production?)
- At the very least, make sure you have a process in place that does not require manual triggering.

Turning Stuff Off

- Be sure to do housekeeping on your systems.
- Turn off
  - obsolete systems **and**
  - unused features.
- Ideally, establish a review process to identify ancient-history systems.

Any question?

Additional info

- https://csirt.egi.eu/2020/10/15/wordpress-security-recommendations/