Experiences and Lessons Learned from a Siemens-Wide Security Patch Management Service for Products

29th Annual FIRST Conference, June 11 - 16, 2017
Manuel Ifland, CISSP
After This Presentation You Will Know …

• … How a Siemens-wide service helps to keep products more secure.

• … That using OSS and COTS components is not a piece of cake.

• … What we should and can do to cope with the challenges.
Why Are We Using OSS and COTS Components?

- Pre-made building blocks
- Faster time-to-market
- Lower development costs
Where There is Light, There is Shadow.

- Products inherit security issues:
  - Vulnerability information is spread all over the Internet
  - Patching is not always an easy task
Siemens Security Vulnerability Monitoring (SVM)

Product / Solution Owner

Components List

Workflow System

Email

PDF

RSS

HTML

XLS

Email

XML

Manual Evaluation

© 2017 Siemens AG & SAFECode
Key Advantages of SVM For Siemens

Confidential information stays in Siemens

Neatly integrates into company’s infrastructure (e.g. SSO, email encryption)
Key Advantages of SVM For Siemens (Cont.)

Dependencies

Security information from sources where support contract is required
Challenges
Challenges

<table>
<thead>
<tr>
<th>Supplement Facts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serving Size: 1 Scoop (3.4g)</td>
</tr>
<tr>
<td>Servings per Container: 10</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Amount Per Serving</th>
<th>% Daily Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>7-Zip 16.04</td>
<td>10 mg</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux Server (v. 7)</td>
<td>200 g</td>
</tr>
<tr>
<td>Foxtit Software Company Foxtit Reader</td>
<td>3 g</td>
</tr>
<tr>
<td>Gimp 2.8.18</td>
<td>8 mg</td>
</tr>
<tr>
<td>Microsoft Office 2013</td>
<td>1 g</td>
</tr>
<tr>
<td>RealVNC VNC 4.1.3</td>
<td>27 mg</td>
</tr>
<tr>
<td>miktex.org MiKTeX 2.9</td>
<td>13 mg</td>
</tr>
<tr>
<td>Oracle Java SE 1.7.0_05</td>
<td>150 mg</td>
</tr>
</tbody>
</table>

**Percent Daily Values are based on a 2,000 calorie diet.

Bill of Materials

Risk Estimation

Names of Third-party Components

© 2017 Siemens AG & SAFECode
Best Practices from SAFECODE Third-party Components Working Group

• Special Interest Group for Third-party Components (TPCs)
• Open Source (OSS) & Commercial off-the-shelf (COTS)
• Various member companies on board:
  • Adobe
  • Boeing
  • Intel
  • Microsoft
  • Siemens
  • Symantec
The Bill of Materials (BOM)

• First and foremost step!

• It depends on where you are in the food chain:

<table>
<thead>
<tr>
<th>Supplement Facts</th>
<th>Amount Per Serving</th>
<th>% Daily Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>T-Zr 15.50</td>
<td>10 mg</td>
<td>1%</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux Server (v. 7)</td>
<td>200 g</td>
<td>20%**</td>
</tr>
<tr>
<td>Food Software Company Food Reader</td>
<td>3 g</td>
<td>1%</td>
</tr>
<tr>
<td>Gimp 2.8.18</td>
<td>8 mg</td>
<td>1%</td>
</tr>
<tr>
<td>Microsoft Office 2013</td>
<td>1 g</td>
<td>11%</td>
</tr>
<tr>
<td>RealVNC VNC 4.1.3</td>
<td>27 mg</td>
<td>1%</td>
</tr>
<tr>
<td>mMax.org MaxTask 2.0</td>
<td>13 mg</td>
<td>1%</td>
</tr>
<tr>
<td>Oracle Java SE 17.5.20</td>
<td>160 mg</td>
<td>6%</td>
</tr>
</tbody>
</table>

* Percent Daily Values are based on a 2,000 calorie diet.
Naming of Third-party Components

- BOM TPCs need to be clearly and uniquely identifiable
- Compatibility with external databases is the key!
Which TPCs Should We Use?

- TPCs are often chosen purely based on functionality
- The following should be considered however:
  - Component Maintenance
  - Development Practices
  - Security Vulnerabilities
  - End of Life
TPC Management Life Cycle – High Level Steps

- Monitor
- Assess
- Mitigate
- Maintain
SDLC and TPC Management Life Cycle
Go Hand in Hand

- Maintain a List of TPCs
- Assess Security Risks from TPCs
- Mitigate or Accept Security Risks from Selected TPCs
- Monitor for Changes in Risk Profiles of TPCs

Flowchart:
- Requirements
- Design
- Develop
- Support
- Verify BOM
Key Takeaways:
Towards Supply Chain Security

OSS and COTS components can increase security risks

Establish a process and perform constant monitoring

Identify components and maintain a BOM
Want to Know More?

Interested in Managing Security for Third Party Components?
Read SAFECODE's new white paper!

http://safecode.org/
http://bit.ly/2qNSdej
Contact

Manuel Ifland, CISSP
Siemens AG
Otto-Hahn-Ring 6
Munich, Germany
manuel.ifland@siemens.com

SAFECODE
Software Assurance Forum for Excellence in Code
401 Edgewater Place, Suite 600
Wakefield, MA 01880
https://safecode.org/
info@safecode.org