Which Kind of SDL Insight Provide Vulnerability Statistics?

Siemens ProductCERT
Rupert Wimmer, 2017-03-02

https://www.siemens.com/cert
Motivation

A Random Vulnerability Statistic

Your Company

W

X

Y

Z
State of the Art: Common Approaches and Their Shortcomings
Here: Total number of vulnerabilities in some Operating Systems

Source: cvedetails.com
State of the Art: Common Approaches and Their Shortcomings

Here: Only Newest Vulnerabilities are Relevant

OS Vulnerabilities in 2015

Source: cvedetails.com
OS Vulnerabilities over time

Source: cvedetails.com
Which Kind of SDL Insight Provide Vulnerability Statistics?
Proper Vulnerability Handling Becomes an Important Part of Digitalization

- Advisories build trust through the consistent, transparent handling of issues
- Digitalization will shift vulnerability handling paradigms of industrial vendors towards the strategy of leading software vendors such as Microsoft, Apple, Oracle…

Published vulnerabilities is 2016 (cvedetails.com)
Vulnerability handling capabilities are only one factor of secure software lifecycle:

<table>
<thead>
<tr>
<th>1. TRAINING</th>
<th>2. REQUIREMENTS</th>
<th>3. DESIGN</th>
<th>4. IMPLEMENTATION</th>
<th>5. VERIFICATION</th>
<th>6. RELEASE</th>
<th>7. RESPONSE</th>
</tr>
</thead>
</table>

Further KPIs for Estimating Security Maturity

2. Establish Security Requirements
   - Security requirements include setup and deployment requirements
     - Are these mentioned in manuals?

4. Perform Security and Privacy Risk Assessments
   - Remaining risks have to be communicated to customers
     - Are these mentioned in manuals?

8. Use Approved Tools

16. Certify Release and Archive
   - Security Tool Vendors like to present their cooperations
     - Any indication of cooperation with security tool vendors?

- Certifications of security ensure a certain level of security
  - Any security certifications for this product?
Conclusion

- Interpretation of vulnerability statistics is tricky.
- Vulnerability Statistics can provide *some* SDL insight.
- Siemens ProductCERT will continue with the transparent vulnerability handling approach.
- For risk and security evaluation, customers will require and request KPIs.
- Siemens ProductCERT encourages to provide and advertise KPIs for SDL insight.
Rupert Wimmer
Siemens ProductCERT
Otto-Hahn-Ring 6
81739 Munich
Germany

Internet
https://siemens.com/cert

E-Mail
productcert@siemens.com

PGP Key Fingerprint:
1C36 704D 88D7 0A12 00B3 1A56 6E75 3C94 F2EB CF9C