SWE-158 - Evaluate Software for Security Vulnerabilities

This version of SWEHB is associated with NPR 7150.2B. Click for the latest version of the SWEHB based on NPR7150.2C

• 1. The Requirement
• 2. Rationale
• 3. Guidance
• 4. Small Projects
• 5. Resources
• 6. Lessons Learned

1. Requirements

3.16.6 The project manager shall ensure that the space flight software systems are assessed for possible security vulnerabilities and weaknesses.

1.1 Notes

NPR 7150.2, NASA Software Engineering Requirements, does not include any notes for this requirement.

1.2 Applicability Across Classes

<table>
<thead>
<tr>
<th>Class</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>CSC</th>
<th>D</th>
<th>DSC</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applicable?</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
</tr>
</tbody>
</table>

Key: ✓ - Applicable | ✗ - Not Applicable

2. Rationale

Space flight software systems are assessed for software and communication security vulnerabilities and weaknesses to ensure such issues are known and managed during the software development life cycle and to ensure the associated risk is also identified and managed.

3. Guidance

The project manager is required to have and implement a Project Protection Plan for their system. The software development organization is responsible for implementing mitigations to address the identified software and communication security vulnerabilities and weaknesses for space flight software systems. It is expected that requirements for these mitigations are generated as security requirements and that those security requirements affecting software are included in the software requirements specification (see SRS). These security requirements are then flowed down and implemented in the design and code and tested by the software development team.

A select group of personnel from the Agency’s Space Protection Working Group (SPWG) actually writes Project Protection Plans and Program Threat Summaries. Program Threat Summaries for NASA are based on similar standardized documents written for national security space systems.

Project managers are to assess their software systems against identified risks (see SWE-156) and agreed to viable security vulnerabilities and weaknesses to confirm that changes required to mitigate or eliminate identified security risks have been implemented in the completed products.

Project managers work with software assurance and other software security experts, including the Information System Security Officer (ISSO), to have software vulnerability assessments performed. Assessments, conducted by software security specialists, may require input from software developers. The results of these assessments may require updates to software requirements to be sure that identified vulnerabilities that can be mitigated in software are properly addressed. It is important for projects to not introduce vulnerabilities and weaknesses by coding for functionality and performance at the expense of security.

Security assessments are performed throughout the project life cycle rather than being performed at the end of the life cycle when it is costly to correct programming errors, bugs, and other identified vulnerabilities. “Continuous test and evaluation of security attributes of systems is an important part of testing as it allows software developers to identify and address vulnerabilities as part of the system architecture and design.” Each project establishes assessment guidelines and frequency suitable to its development life cycle or follows any existing Center guidelines, tailored appropriately for the project.

Quality, security-related vulnerability assessments/analyses:

• Include newly developed code and, to the extent possible, off-the-shelf (OTS), open source, and reused code.
• May focus on 484:
  • Code that runs by default.
  • Code that runs in elevated context.
  • Code connected to a globally accessible network interface.
  • Code written in a language whose features facilitate building in vulnerabilities.
  • Code with a history of vulnerabilities.
- Code that handles sensitive data.
- Complex code.
- Code that changes frequently.
- Assess for bugs, programming errors, and potential failures.
- Confirm, to some acceptable level of rigor, that software does not do what it is not supposed to do.
- Assess the impact and likelihood of vulnerability exploitation.
- May check for adherence to secure architecture, design, coding standards, including the use of secure coding practices (may be difficult to do for OTS software).
- May use automated security static code analysis as well as coding standard static analysis.

```
NASA users should consult center Process Asset Libraries (PALs) for center-specific guidance and resources related to software security.
```

Additional guidance related to software security may be found in the following related requirements in this Handbook:

<table>
<thead>
<tr>
<th>SWE-027</th>
<th>Use of Commercial, Government, and Legacy Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>SWE-135</td>
<td>Static Analysis</td>
</tr>
<tr>
<td>SWE-154</td>
<td>Identify Security Risks</td>
</tr>
<tr>
<td>SWE-155</td>
<td>Implement Risk Mitigations</td>
</tr>
<tr>
<td>SWE-156</td>
<td>Evaluate Systems for Security Risks</td>
</tr>
<tr>
<td>SWE-157</td>
<td>Protect Against Unauthorized Access</td>
</tr>
<tr>
<td>SWE-159</td>
<td>Verify and Validate Risk Mitigations</td>
</tr>
</tbody>
</table>

4. Small Projects

No additional guidance is available for small projects.

5. Resources

```
Click here to view master references table.
```

- (SWEREF-064)
  Engineering Principles for Information Technology Security (A Baseline for Achieving Security), NIST SP 800-27, Revision A.

- (SWEREF-065)
  Security Considerations in the System Development Life Cycle, NIST SP 800-64 Revision 2.

- (SWEREF-082)
  NASA Space Flight Program and Project Management Requirements, w/Changes 1-16 NPR 7120.5E, NASA Office of the Chief Engineer, 2012. Effective Date: August 14, 2012, Expiration Date: August 14, 2019

- (SWEREF-273)

- (SWEREF-482)

- (SWEREF-483)

- (SWEREF-484)

- (SWEREF-485)
5.1 Tools

Tools relative to this SWE may be found in the table below. You may wish to reference the Tools Table in this handbook for an evolving list of these and other tools in use at NASA. Note that this table should not be considered all-inclusive, nor is it an endorsement of any particular tool. Check with your Center to see what tools are available to facilitate compliance with this requirement.

<table>
<thead>
<tr>
<th>Tool name</th>
<th>Type</th>
<th>Owner/Source</th>
<th>Link</th>
<th>Description</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sonatype</td>
<td>COTS</td>
<td>Sonatype, Inc.</td>
<td><a href="https://www.sonatype.com/">https://www.sonatype.com/</a></td>
<td>Software supply chain management where it scans for known vulnerabilities when using open source software (for ground systems/networks).</td>
<td>IV&amp;V</td>
</tr>
<tr>
<td>OWASP Dependency Check</td>
<td>Open Source</td>
<td>Open Web Application Security Project (OWASP)</td>
<td><a href="https://www.owasp.org/index.php/MainPage">https://www.owasp.org/index.php/MainPage</a></td>
<td>Software supply chain management where it scans for known vulnerabilities when using open source software (for ground systems/networks).</td>
<td>IV&amp;V</td>
</tr>
<tr>
<td>Metasploit Express/Pro</td>
<td>COTS</td>
<td>Rapid7</td>
<td><a href="https://www.metasploit.com/">https://www.metasploit.com/</a></td>
<td>Penetration testing for ground systems/networks.</td>
<td>IV&amp;V</td>
</tr>
<tr>
<td>Fortify</td>
<td>COTS</td>
<td>MicroFocus</td>
<td><a href="https://software.microfocus.com/en-us/products/static-code-analysis-sast/overview">https://software.microfocus.com/en-us/products/static-code-analysis-sast/overview</a></td>
<td>MicroFocus Fortify is a static code analysis tool that is used to scan software for security vulnerabilities. Fortify is used extensively through the DoD community. GSFC uses Fortify for its DOD Clients. The NASA OCIO procured an enterprise license of Fortify. Please contact the SOC for more information <a href="mailto:soc@nasa.gov">soc@nasa.gov</a>.</td>
<td>GSFC</td>
</tr>
<tr>
<td>BlackDuck Hub</td>
<td>COTS</td>
<td>Black Duck Software, Inc.</td>
<td><a href="https://www.blackducksoftware.com/products/hub">https://www.blackducksoftware.com/products/hub</a></td>
<td>Software supply chain management where it scans for known vulnerabilities when using open source software (for ground systems/networks). A Complete Open Source Management Solution - Fully discover all open source in your code - Map components to known vulnerabilities - Identify license compliance and component quality risks - Set and enforce open source policies - Integrate open source management into your DevOps environment - Monitor and alert when new threats are reported</td>
<td>IV&amp;V</td>
</tr>
</tbody>
</table>

6. Lessons Learned

No Lessons Learned have currently been identified for this requirement.