6. Elevation of Privilege

Question

What is elevation of privilege? How does authorization mitigate this threat?

Answer

An elevation of privilege threat is aimed at obtaining privileged access to resources for gaining unauthorized access to information or to compromise a system.\(^1\)

Elevation of privilege results from giving an attacker authorization permissions beyond those initially granted. For example, an attacker with a privilege set of "read only" permissions somehow elevates the set to include "read and write."\(^2\)

Authorization is the process of granting or denying access to a system resource. Most computer security systems are based on a two-step process. The first stage is authentication, which ensures that a user is who he or she claims to be. The second stage is authorization, which allows the user access to various resources based on the user's identity.\(^3\)

Prevent elevation of privilege attacks by ensuring:

- There are authorization mechanisms in place.
- The application has clearly defined the user types and the rights of said users.
- There is a least privilege stance \(^5\) in operation.
- The authorization mechanisms work properly, fail securely, and cannot be circumvented.
- Authorization is checked on every request.
- Development/debug backdoors are not present in production code.

Mitigations for Specific Threats

<table>
<thead>
<tr>
<th>Summary: Elevation of privilege types of threats occur when an attacker is able to gain elevated access rights through unauthorized means, in this case a process may be vulnerable to cross-site request forgery (CSRF or XSRF). More information on CSRF may be found here.(^6)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recommendations: Recommended mitigations include requiring that all authenticated state-changing requests include an additional piece of secret payload (canary or CSRF token) which is known only to the legitimate web site and the browser and which is protected in transit through SSL/TLS. Audit comments should indicate what protections are in use against cross-site request forgery or why they are unnecessary for the indicated data flow (such as no state changing requests are made across the data flow).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Summary: Elevation of privilege types of threats occur when an attacker is able to gain elevated access rights through unauthorized means, in this case an attacker may pass data into a process in order to change the flow of program execution within the process to the attacker's choosing.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recommendations: As this is a threat of subverting any authentication and authorization mechanisms in place, those mechanisms may not be used to mitigate this threat. Mitigations for this threat prevent bypassing those mechanisms. Such mitigations may include:</td>
</tr>
<tr>
<td>• Appropriate input validation and exception handling to avoid unexpected execution paths</td>
</tr>
<tr>
<td>• Guarding against buffer overflows and other memory management issues</td>
</tr>
<tr>
<td>• Defaulting to least privilege</td>
</tr>
<tr>
<td>• Protecting authentication and authorization paths. For example, if authentication and authorization is dependent upon database data, code paths that interact with the database must be protected to ensure the integrity of that data.</td>
</tr>
</tbody>
</table>
**Summary:** Elevation of privilege types of threats occur when an attacker is able to gain elevated access rights through unauthorized means, in this case an external entity may be able to remotely execute code for a process.

**Recommendations:** While the external entity should protect itself against remote code execution, the process should take care not to pass any potentially executable data to the external entity. Therefore, mitigations include:

- Limit the amount of user provided data sent to the external entity
- User provided data that must be provided to the external entity should be validated and restricted as much as possible

---

**Summary:** Elevation of privilege types of threats occur when an attacker is able to gain elevated access rights through unauthorized means, in this case a process may be able to remotely execute code for an external entity.

**Recommendations:** For this threat to be applicable, the indicated process must execute input from the indicated interaction that has not been validated. Therefore, recommended mitigations include:

- The process does not contain any paths which execute input data from the data flow
- If a process does execute the input data then the data should be validated in a manner which would preclude arbitrary code to be executed

---

**References**

1. OWASP: Application Threat Modeling
2. MSDN: Elevation of Privilege
3. Webopedia: Definition of authorization
4. OWASP: Application Threat Modeling
5. US-CERT: Principle of Least Privilege
6. Cross-Site Request Forgery, OWASP