Rec. 10. Environment (ENV)

- ENV01-C. Do not make assumptions about the size of an environment variable
- ENV02-C. Beware of multiple environment variables with the same effective name
- ENV03-C. Sanitize the environment when invoking external programs

Information for Editors
In order to have a new guideline automatically listed above be sure to label it env and recommendation.

Risk Assessment Summary

<table>
<thead>
<tr>
<th>Rule</th>
<th>Severity</th>
<th>Likelihood</th>
<th>Remediation Cost</th>
<th>Priority</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENV01-C</td>
<td>High</td>
<td>Likely</td>
<td>Medium</td>
<td>P18</td>
<td>L1</td>
</tr>
<tr>
<td>ENV02-C</td>
<td>Low</td>
<td>Unlikely</td>
<td>Medium</td>
<td>P2</td>
<td>L3</td>
</tr>
<tr>
<td>ENV03-C</td>
<td>High</td>
<td>Likely</td>
<td>High</td>
<td>P9</td>
<td>L2</td>
</tr>
</tbody>
</table>

Related Rules and Recommendations

ENV00-J. Do not sign code that performs only unprivileged operations
ENV01-C. Do not make assumptions about the size of an environment variable
ENV01-J. Place all security-sensitive code in a single JAR and sign and seal it
ENV02-C. Beware of multiple environment variables with the same effective name
ENV02-J. Do not trust the values of environment variables
ENV03-C. Sanitize the environment when invoking external programs
ENV03-J. Do not grant dangerous combinations of permissions
ENV04-J. Do not disable bytecode verification
ENV05-J. Do not deploy an application that can be remotely monitored
ENV06-J. Production code must not contain debugging entry points
ENV30-C. Do not modify the object referenced by the return value of certain functions
ENV31-C. Do not rely on an environment pointer following an operation that may invalidate it
ENV32-C. All exit handlers must return normally
ENV33-C. Do not call system()
ENV34-C. Do not store pointers returned by certain functions

Rec. 10. Environment (ENV)
Rule 10. Environment (ENV)
Rule 16. Runtime Environment (ENV)