|  |  |  |
| --- | --- | --- |
| Base Finding | Technical Impact (TI) | The potential result that can be produced by the weakness, assuming that the weakness can be successfully reached and exploited. |
| Base Finding | Acquired Privilege (AP) | The type of privileges that are obtained by an attacker who can successfully exploit the weakness. |
| Base Finding | Acquired Privilege Layer (AL) | The operational layer to which the attacker gains privileges by successfully exploiting the weakness. |
| Base Finding | Internal Control Effectiveness (IC) | the ability of the control to render the weakness unable to be exploited by an attacker. |
| Base Finding | Finding Confidence (FC) | the confidence that the reported issue is a weakness that can be utilized by an attacker |
| Attack Surface | Required Privilege (RP) | The type of privileges that an attacker must already have in order to reach the code/functionality that contains the weakness. |
| Attack Surface | Required Privilege Layer (RL) | The operational layer to which the attacker must have privileges in order to attempt to attack the weakness. |
| Attack Surface | Access Vector (AV) | The channel through which an attacker must communicate to reach the code or functionality that contains the weakness. |
| Attack Surface | Authentication Strength (AS) | The strength of the authentication routine that protects the code/functionality that contains the weakness. |
| Attack Surface | Level of Interaction (IN) | the actions that are required by the human victim(s) to enable a successful attack to take place. |
| Attack Surface | Deployment Scope (SC) | Whether the weakness is present in all deployable instances of the software, or if it is limited to a subset of platforms and/or configurations. |
| Environmental | Business Impact (BI) | The potential impact to the business or mission if the weakness can be successfully exploited. |
| Environmental | Likelihood of Discovery (DI) | The likelihood that an attacker can discover the weakness |
| Environmental | Likelihood of Exploit (EX) | the likelihood that, if the weakness is discovered, an attacker with the required privileges/authentication/access would be able to successfully exploit it. |
| Environmental | External Control Effectiveness (EC) | the capability of controls or mitigations outside of the software that may render the weakness more difficult for an attacker to reach and/or trigger. |
| Environmental | Prevalence (P) | How frequently this type of weakness appears in software. |

External Control Effectiveness (EC), which is part of the Environmental group, is the capability of controls, or mitigations, outside of the software that may render the weakness more difficult for an attacker to reach and/or trigger. EC will always fall between 0 and 1 based on its code. The lower the score, the easier the path for the attacker. The codes carry a weight as follows:

* None - 1.0 - No controls exist.
* Limited - 0.9 - There are simplistic methods or accidental restrictions that might prevent a casual attacker from exploiting the issue.
* Moderate - 0.7 - The protection mechanism is commonly used but has known limitations that might be bypassed with some effort by a knowledgeable attacker.
* Indirect (Defense-in-Depth) - 0.5 - The control does not specifically protect against exploitation of the weakness, but it indirectly reduces the impact when a successful attack is launched, or otherwise makes it more difficult to construct a functional exploit.
* Best-Available - 0.3 - The control follows best current practices, although it may have some limitations that can be overcome by a skilled, determined attacker, possibly requiring the presence of other weaknesses. For example, Transport Layer Security (TLS) / SSL 3 are in operation throughout much of the Web, and stronger methods generally are not available due to compatibility issues.
* Complete - 0.1 - The control is completely effective against the weakness, i.e., there is no bug or vulnerability, and no adverse consequence of exploiting the issue. For example, a sandbox environment might restrict file access operations to a single working directory, which would protect against exploitation of path traversal. A non-zero weight is used to reflect the possibility that the external control could be accidentally removed in the future, e.g. if the software's environment changes.
* Default- 0.6 - The median of Complete, Best-Available, Indirect, Moderate, Limited, and None.
* Unknown - 0.5 - There is not enough information to provide a value for this factor. Further analysis may be necessary. In the future, a different value might be chosen, which could affect the score.
* Not Applicable - 1.0 - This factor is being intentionally ignored in the score calculation because it is not relevant to how the scorer prioritizes weaknesses.

The EnvironmentalSubscore is calculated as:

[ (10\*BusinessImpact + 3\*LikelihoodOfDiscovery + 4\*LikelihoodOfExploit + 3\*Prevalence) \* f(BusinessImpact) \* ExternalControlEffectiveness ] / 20.0

Example of an Environmental Subscore:

Business Impact (BI) = **0.6** (Medium)

Likelihood of Discovery (DI) = **1.0** (High)

Likelihood of Exploit (EX) = **0.5** (Unknown)

External Control Effectiveness (EC) = **0.5** (Indirect)

Prevalence (P) = **0.9**

Business Impact (BI) = **1.0**

Math:

[ (10 \* 0.6) + (3 \* 1.0) + (4 \* 0.5) + (3 \* 0.9) \* 1 \* 0.5] / 20.0

[ (6) + (3) + (2) + (2.7) \* 1 \* 0.5] / 20.0

[ (13.7) \* 1 \* 0.5] / 20.0

[ 6.85] / 20.0 = 0.3425

Environmental Subscore = **0. 3425**

Reference:

CWE Common Weakness Enumeration. (n.d.). Retrieved August 22, 2020. Retrieved from CWE.Mitre.org: https://cwe.mitre.org/cwss/cwss\_v1.0.1.html#2.1