**Severity Level Inform**

**General**

The common core categories are High, Medium, and Low, with additional categories being added over time, such as Critical, Lowest, Informational (or Informative/Info), and Unknown. High and Low are equivalent to Major and Minor. Other supplementary categories include Governance, Optimizations, Resolved, Gas Optimization, Code Style and Best Practice, and Weakness or Suggestion. **Hacken io** is the only one whose **severity levels are based on a mathematical formula. Peckshield** bases its **severity levels on "Impact + Likelihood," following the OWASP Risk Rating Methodology.** **ChainSecurity and SolidProof base their classification on the CVSS version 3.0 risk rating methodology. Severity is determined by considering both likelihood and impact. Additionally SolidProof s**everity Level is accompanied by complementary metrics such as Action Required and a value scale from 1 to 10. Finally, Trail of Bits radically changed their classification system, expanding from 4 to 8 categories: Strong, Satisfactory, Moderate, Weak, Missing, Not Applicable, Not Considered, and Further Investigation Required.

**Details by company**

**Beosin.** Beosin started operations in [year]. Its first public reports only included the vulnerabilities found and their status (pass). In 2020, they began using their own categories (coding, general, and business security) to group vulnerabilities. From 2022 onward, up to the latest audited report, they integrated the categories critical, high, medium, low, and info into their audit reports. However, **the meaning of each of these categories has not been published**

**Calisto Network.** Calisto Network has always used the categories high, medium, and low to classify vulnerabilities. However, **the meaning of these categories is not publicly available**

**ChainSecurity.** Since 2018 and up to the latest report reviewed in 2024, Chain Security has consistently used the categories critical, high, medium, and low. **This classification is based on the CVSS risk rating methodology. Severity is determined by considering both likelihood and impact.** Likelihood refers to the probability of a security vulnerability being encountered or exploited in the wild, while impact specifies the technical and business-related consequences of an exploit

**Coinsult** uses the categories Informational, Low-Risk, Medium-Risk, and High-Risk

**ContractWolf** uses the categories critical, major, medium, minor, and informational in 2023, and in 2025 **they introduced a new category called resolved.**

**CyberScope.** CyberScope uses the categories critical, medium, minor or informative. However, **the meaning of these categories is not publicly available**

**EtherAuthority** uses the categories critical, high, medium, low and Lowest / Code Style/ Best practice. They introduced a **new category that includes code style and best practice: Lowest / Code Style / Best Practice.**

**FreshCoins** uses the categories high, medium, low and optimizations and Informational. **They introduced a new category called optimizations.** However, **the meaning of these categories is not publicly available.**

[**Hacken.io**](http://hacken.io) **removed the Informational category** that it used in 2023 and is currently using the categories High, Medium, Low, and Critical. It is also important to highlight that this company is the only one whose **severity levels are based on a mathematical formula,** a vulnerability severity formula based on four key metrics: Likelihood, Impact, Complexity, and Exploitability. More information can be found here: <https://github.com/hknio/severity-formula/blob/main/README.md>

**Hashex** used the categories Critical, High, Medium, and Low, and now **they have added a new category called Info.**

**interFiAudits** changed the category High to Major, Low to Minor, and **added a new category called unknown.**

**Omniscia** used medium, informational, minor, major and **added a new category called unknown.**

**Paladin** used high, medium, low, informationa**l and added a new category called governance**

**Peckshield** bases its **severity levels on "Impact + Likelihood," following the OWASP Risk Rating Methodology.** However, **the meaning of these categories is not publicly available**

**QuillAudit** started with the categories High, Medium, and Low, and in its most recent reports**, it added the Informational category.**

**Sherlock** **does not disclose the meaning of its classification categories:** High, Medium, Low, and Informational.

**SlowMist has introduced two new categories: Weakness and Suggestion.**

**SolidProof** also bases the definitions of its categories on the concept that risk represents the probability that a certain threat source will exploit a vulnerability, and the impact of that event on the organization or system. **Risk Level is computed based on CVSS version 3.0.** Additionally, the Severity Level is accompanied by complementary metrics such as Action Required and a value scale from 1 to 10.

**Spearbit,** in addition to the common categories Critical, High, Medium, and Low, also **includes Gas Optimization and Informational.**

**Trail of Bits** initially used the categories High, Medium, Low, Informational, and Undetermined. In 2024, they radically changed their classification system, expanding from 4 to 8 categories: Strong, Satisfactory, Moderate, Weak, Missing, Not Applicable, Not Considered, and Further Investigation Required.

**Zellic**  does **not disclose the meaning of its classification categories**

**Socken** removed the severity classification definitions from their reports