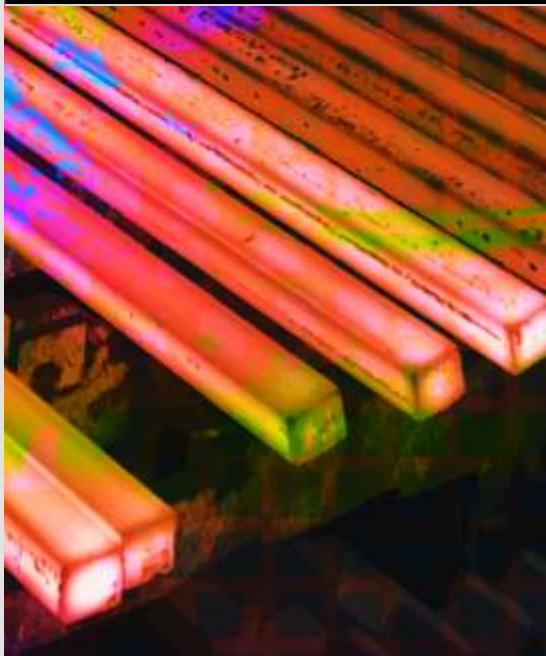
Carnegie Mellon University
Software Engineering Institute

Fix What First? Using SSVC to Prioritize Vulnerability Response



APRIL 2023

Leigh Metcalf

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

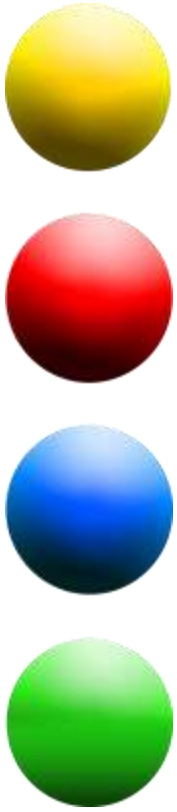
DM23-0382

Motivation

We propose a Stakeholder-Specific Vulnerability Categorization (SSVC) as an improvement.

- Focus is on *decisions*, not technical severity
- Transparent, role-specific recommendations
- Experiment design-to-test process consistency
  - Thanks to my co-authors, conference attendees, and GitHub contributors who have helped improve SSVC so far.
- Communication between analysts and risk managers
  - Analysts know what the risk manager chooses.
  - Risk managers know what analysts will decide on vuls consistently.

Motivation



We propose a Stakeholder-Specific Vulnerability Categorization (SSVC) as an improvement.

- Focus is on *decisions*, not technical severity
- Transparent, role-specific recommendations
- Experiment design-to-test process consistency
  - Thanks to my co-authors, conference attendees, and GitHub contributors who have helped improve SSVC so far.
- Communication between analysts and risk managers
  - Analysts know what the risk manager chooses.
  - Risk managers know what analysts will decide on vuls consistently.

SSVC Contributions

1. Decision process and descriptions that could be used to make vulnerability management decisions
2. Method for how a justifiable decision process and descriptions can be constructed, adapted, and tested

1) is valuable, and though we're on [version 2](), it is always improving
2) is perhaps more important because it lets you adapt

Development and improvement are ongoing.

If you have suggestions, tell us!
https://github.com/CERTCC/SSVC

SSVC Contributions

1. Decision process and descriptions that could be used to make vulnerability management decisions
2. Method for how a justifiable decision process and descriptions can be constructed, adapted, and tested

1) is valuable, and though we're on [version 2](), it is always improving
2) is perhaps more important because it lets you adapt

Development and improvement are ongoing.

If you have suggestions, tell us!
https://github.com/CERTCC/SSVC

SSVC Contributions

1. Decision process and descriptions that could be used to make vulnerability management decisions
2. Method for how a justifiable decision process and descriptions can be constructed, adapted, and tested

1) is valuable, and though we're on version 2, it is always improving
2) is perhaps more important because it lets you adapt

Development and improvement are ongoing.

If you have suggestions, tell us! https://github.com/CERTCC/SSVC

Contact Information

Leigh Metcalf
Senior Network Security
Research Analyst

Telephone: +1 412.268.8591
Email: info@sei.cmu.edu