

# Fix What First? Using SSVC to Prioritize Vulnerability Response

**APRIL 2023**

Leigh Metcalf



# Document Markings

Copyright 2023 Carnegie Mellon University.

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.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

CERT® and CERT Coordination Center® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

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

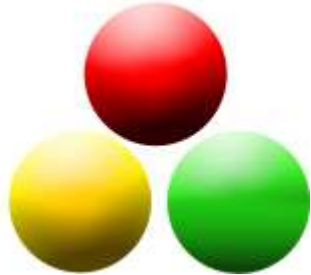
Development and improvement are ongoing.

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](mailto:info@sei.cmu.edu)