



Update on
ISO29147
working draft



Damir Rajnovic – Gaus <gaus@cisco.com>
PSIRT Incident Manager

Current status

- ISO29147 “Responsible Vulnerability Disclosure”
- Currently in the 2nd Working Draft
- Next meeting will be in early May in Beijing, China

Changes from the 1st working draft

- The document should be applicable to all manufacturers (software, hardware, cars, trains, transformers, etc.)
- Focus is only on interfaces between vulnerability finders, vendors and users
- Vendor's internal processes and procedures are out of the scope

Projected future actions and timeline

- The 2nd working draft is still largely unpolished
- Many details are still not in place
- The document may have additional 2-3 drafts
- It may be ready for voting in 1½ - 2½ years

Challenges

- ISO relies on physical presence during editing sessions
- There is no mechanism in place to officially work with ISO in between face-to-face meetings. Progress is limited to biyearly tempo.

Internet
Infrastructure
Vendors
Special Interest
Group



About Vendor SIG

- Internet Infrastructure Vendors Special Interest Group operates under FIRST (Forum of Incident Response and Security Teams) umbrella (<http://www.first.org/vendor-sig/>)
- Vendor SIG is a forum for vendor's teams that handle security vulnerabilities in their respective products
- Currently 29 participating vendors

Vendor SIG activities

- Learn from each other, share best practices
- Facilitate information sharing among members
- Formulate industry position on common issues

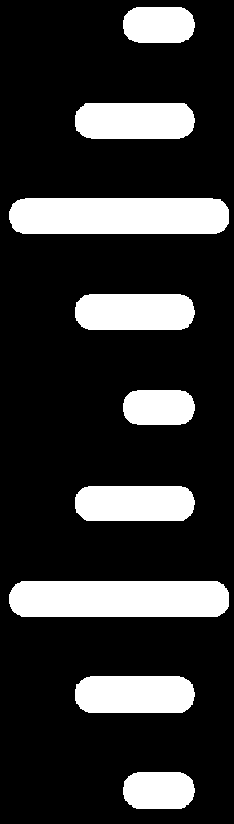
Guidelines for Vendor-Coordinator relationship

ISO standards

ENISA studies

Invitation

- We invite you to FIRST Annual Conference to join Vendor SIG meeting and the rest of FIRST conference
- The meeting will take place in the period Jun-28 – Jul-03 in Kyoto, Japan (see <http://conference.first.org/> for all details)



cisco