January 20, 2017 Leave a Comment

Security

# Guidelines and Practices for Multi-Party Vulnerability Coordination Open to Review

Omar Santos

Recent cyber attacks on organizations around the world have demonstrated the need for consistency in managing security vulnerabilities. To answer that demand, the Industry Consortium for the Advancement of Security on the Internet (ICASI) and the Forum of Incident Response and Security Teams (FIRST) created the FIRST Vulnerability Coordination Special Interest Group (SIG). This is a collaboration among vendors, security researchers, product security incident response teams (PSIRTs), computer security incident response teams (CSIRTs), and other stakeholders in the incident response community. One of the goals for the Vulnerability Coordination SIG is to "develop and publish vulnerability coordination best practices, which include use cases or examples that describe scenario and disclosure paths".

But the best way for this initiative to be successful is for those who live and breathe this work every day to provide insight. As such, the Vulnerability Coordination SIG has recently made available a provisional draft of the Guidelines and Practices for Multi-party Vulnerability Coordination for public comment. This paper was created in collaboration with the United States Department of Commerce National Telecommunications and Information Administration (NTIA), which also endorsed the effort.

The paper covers five different use cases including different security vulnerability coordination scenarios. It also provides several guiding concepts and best practices for incident response teams, including:


The final draft of the paper is open to public comment through January 31, 2017. Comments should be submitted by email to vulcoord-sig-comments@first.org. After the comment period is closed, the Vulnerability Coordination SIG will revise the document and publish a final version.

As a matter of policy, Cisco takes security vulnerabilities very seriously and continues to take active measures to safeguard the security and reliability of our equipment. We maintain a very open relationship with the security research community and view this collaborative relationship as vital to helping protect our customers' networks. Working with industry peers, security researchers, and incident response teams on cooperative efforts like Vulnerability Coordination SIG enhance the way we collectively protect our customers while coordinating, disclosing and fixing security vulnerabilities.

Share

Share:

Tags: FIRST icasi ntia psirt security vulnerabilities vulnerability coordination

CONNECT WITH CISCO

- 
- 
- 