

## Responsible Vulnerability Disclosure panel

The viewpoint of an IT security research and IT security software vendor (1996-2008)

*Iván Arce - CTO*

.....

Core Security Technologies  
Humboldt 1967 2do Piso  
Buenos Aires, Argentina  
Phone: (+54-11) 5556-2673  
Email: [ivan.arce@coresecurity.com](mailto:ivan.arce@coresecurity.com)

Who is this guy?

---

..... **CORE SECURITY TECHNOLOGIES** .....

- **CTO and co-founder of Core Security Technologies**  
**(<http://www.coresecurity.com>)**
  - Founded 1996 in Buenos Aires, Argentina, involved in security research and vulnerability discovery ever since
  - Early adopters and pioneers of the public disclosure process of software bugs (mid 1990s)
  - 80+ security advisories, papers and technical articles published. Several hundredths of bugs reported. Coordinated bug reports with Microsoft, Cisco, Sun, SGI, IBM, Digital, HP, all Linux vendors, BSD, etc.
  - **In 2008: WonderWare SuiteLink DoS & CitectSCADA ODBC buffer overflow**
- **CORE is also a software vendor:** Develops and sells the first commercial software package for automated security testing that includes real exploit code: CORE IMPACT.
- Provides security consulting services: Network/Application penetration testing, source code and black box security audits. **Found and reported thousands of bugs over the past 13 years.**

## Why do we do vulnerability research & disclosure?

### ..... **VULNERABILITY RESEARCH, REPORTING & DISCLOSURE** .....

- **End goal is to help vulnerable user organizations understand and mitigate risk**
- **NOT A REVENUE GENERATION ACTIVITY**
- **Knowledge acquisition & transfer; to improve our individual and team skills**
- **Information security professional imperative**
- **Advancement of the discipline in a scientific manner**
- **Public safety/welfare issue**
- **Brand & name recognition**

## How do we do vulnerability research & disclosure?

### ..... OUR BASIC PROCEDURE .....

- **Dedicated team (4) for management of the report and disclosure process**
- **Discoverers/Researchers are not dedicated to task (part-time activity) and belong to other teams (Basic research, SCS, Engineering, QA, SE, etc.)**
- **Discoveres/Researchers are de-coupled from the Security Advisories team**
- **Software vendor is always notified first. This is a courtesy not an obligation.**
- **A coordinated release is always attempted but not always possible.**
- **Conceived as a risk management process. The risk of exploitation increases over time.**
- **Other stakeholders are also entitled to provide mitigating solutions.**
- **Infosec professionals require precise and accurate technical details to assess risk.**
- **Coordination with external entities only when necessary.**

# Which guidelines do we follow during the vulnerability reporting & disclosure?



## ..... OUR BASIC GUIDELINES .....

- The applicable laws and contractual obligations supersede guidelines and internal policies
- There is no silver bullet, one-size doesn't fit all
- Enforce process transparency. Document and publish communications between stakeholders.
- Assume independent discovery. Minimize time to disclosure.
- Assume exploitable unless extensive and detailed research "proves" otherwise. Be conservative, assume worst-case scenario.
- Be tolerant and flexible during the process but estimate likelihood of completion.
- Publish enough technical details to facilitate accurate and precise assessment of risk.
- Research and publish potential workarounds and alternative mitigation strategies. Patching is not the only possible way to address software security bugs and the official vendor is not the only possible solution provider.
- Keep in mind that monitoring, prevention, containment and auditing are also important.
- Do not bias or discriminate access to information on the basis of financial capabilities, geographical boundaries, moral prejudice or presumed ethical stances, etc.