Executive Perspective

# Vulnerability Disclosure

**By John N. Stewart**

As a customer, you most likely want to learn about technology vulnerabilities in your information systems as soon as possible. With that knowledge alone, you might then be able to take steps to minimize the risk to your information system while awaiting a fix from the vendor. On the other hand, would you want *everyone* to know about a vulnerability in the technology you're using? Vendors have the same dilemma: by disclosing vulnerabilities without fixes in their technology, they alert not only their customers, but then risk your networks by also alerting those who exploit vulnerabilities for their own gain.

To address vulnerabilities effectively, vendors must work in conjunction with the research community to fully understand vulnerabilities as they are discovered, to develop solutions, and to disclose information to customers in ways that best mitigate risk. Exactly when and how to disclose information system vulnerabilities and their fixes can be controversial questions, but just as with protecting non-IT and physical infrastructure, there are best practices and trends regarding the management of vulnerabilities. Software is complex, with increasing dependencies on third-party software programs. How we manage vulnerabilities in that software is therefore a very important part of managing information systems risk.

## Cooperative Disclosure

The research community and vendors have some common goals: reducing the risks to information systems and stopping related malicious activity. Remaining mindful of these goals can help all sides—vendor, researcher, and customer—remember another common goal: to minimize the impact of vulnerabilities on customers.

It is in the best interest of customers that the vendor and research communities work cooperatively. Vendors need to be open to input from researchers, work with them to fully understand their discoveries and their concerns, and give them attribution when disclosure is made if the researcher so desires. Researchers should understand and appreciate the challenges vendors face in developing fixes for vulnerabilities, especially when that involves extensive testing using third-party programs.

In short, both sides need to find a forum to collaborate, air differences of opinion as required, and continue understanding each others' positions as they change over time.

## Roles in the Framework

If both vendors and researchers want to do what is best for the vendors' customers, their mutual goal might best be served by working within a framework that facilitates communication, research, and disclosure. Many vendors and researchers have already agreed to the Vulnerability Disclosure Framework published by the National Infrastructure Advisory Council (NIAC) in January 2004. Its purpose is to represent the best practices for everyone involved. Vendors and researchers should adhere to a framework such as this or work collaboratively to drive improvement through a similar structured forum.

Vendor responsibilities include continued improvement in development and testing processes. Vendors should collaborate with the research community, remaining open to vulnerability discovery from external parties. And

vendors need a robust process for managing that collaboration to ensure that discoveries are properly addressed, disclosed, and credited.

Researchers should collaborate with vendors, working toward the common goal of providing solutions that allow for timely resolution of vulnerabilities and a disclosure framework that minimizes risk of exploitation.

End users—the customers who use software products every day—also have an important role as the high rate of technology innovation continues. As customers demand more complex networks with shorter implementation cycles to remain competitive, methods used to breach information systems advance at a similar pace. Customers must budget and plan for ongoing maintenance of their information systems.

## Succeeding in the Future

Most companies today operate with software from multiple vendors, and therefore they have to deal with cross-vendor dependencies and testing. Those who succeed in this arena must draw on the experience gained in the last 10 years to create more effective means of system design, engineering, testing, and discovery and disclosure of vulnerabilities.

As business networks grow in complexity, researchers and vendors will not stop creating new and more effective defenses against network-based attacks and crimes. Along with advances in products and systems, innovation will continue in vulnerability disclosure as well.

Looking ahead, differences of opinion are inevitable, but collaboration is essential. To do otherwise is to miss opportunity.

## About the Author

John N. Stewart is Vice President and Chief Security Officer, Corporate Security Programs Organization, at Cisco Systems, Inc.


**Corporate Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

**European Headquarters**
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

**Asia Pacific Headquarters**
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799


Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Web site at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe




XXXX_ETMG_XX_10.04

Printed in the USA