

As of April 22, 20

- HOME
- ALL STORIES
- LATEST NEWS
- COLUMNS
- OPINIONS
- GUEST VIEWS
- SHORT TAKES
- DATA WATCH
- SPECIAL REPORTS
- ZEICHICK'S TAKE
- SD TIMES 100
- EDITORS' BLOG
- RSS FEEDS
- FACEBOOK
- TWITTER
- RESOURCES**
- WHITE PAPERS
- SPONSORED PROFILES
- JOB BOARD
- WEBINAR CENTER

HOME >> LATEST NEWS

Holding ISVs to a Higher Security Standard

Turning up the heat means better software.

By Jennifer deJong

February 5, 2008 —

Your brand new sweater has a hole in it. The coffee maker you got for Christmas doesn't power up when you plug it in.

No problem. A refund or replacement, and perhaps even an apology, is in order.

But what about that security defect you found in the software you licensed last month?

Sorry, the user of that software, not the company that makes it, is left holding the bag.

"That's a terrible way to do things," said Brian Chess, co-founder and chief scientist of application security toolmaker Fortify. "It's troublesome to shift the burden of security to the customer."

But that is where the responsibility lies today. When security flaws—essentially poorly

Printable version

Most Read Latest News Blog Resources

Weighing in on Visual Studio 2010

Experts talk about what they like about the newly released platform, and what they want to...

Is code escrow for SaaS making a comeback?

Though the practice has fallen out of widespread usage, some software companies are explor...

An augmented view of reality

Augmented Reality is just entering the mobile marketplace, but what can it do and what pot...

SEND TO A FRIEND

- Technorati
- Digg
- Reddit
- Slashdot
- Facebook
- Friendfeed
- Twitter
- del.icio.us
- ShareThis

FEEDBACK

13+

data quality to for developers

click here to download your free trial

1-800-MELISSA **MELISSA**

- News on Monday**
[more>>](#)
- SharePoint Tech Report**
[more>>](#)

FREE SOFTWARE

BZ RESEARCH

ALM

SHAREPOINT

EVENTS CALENDAR

PRINT/PDF EDITION

PRINT/PDF BACK ISSUES

SERVICES

SUBSCRIBE TODAY

CUSTOMER SERVICE

EDITORIAL CALENDAR

EDITORIAL BEATS

GUEST VIEW GUIDE

SD TIMES 100 GUIDE

EVENTS CALENDAR

ADVERTISING

ARTICLE REPRINTS

REPORT A BUG

SITE MAP

BZ MEDIA

ABOUT US

BZ MEDIA NEWS

BZ RESEARCH

SYSMANNEWS

SPTECHCON

iPHONE/iPAD DEVCON

PRIVACY POLICY

CONTACT US

constructed code that makes it possible for hackers to steal sought-after data such as credit card numbers— are found in software written in-house, a developer can move quickly to rework the code. But when the vulnerability identified is in an application licensed from an independent software vendor, IT professionals can't go it alone, because they don't have access to the application's source code.

"You say to the vendor: 'Hey, guys, you have got to fix this in the next release,'" said Mandeep Khara, vice president of marketing of application security toolmaker Cenzic. But that could take three months, or even six, he said. "You get the patch when you get the patch."

In the meantime, IT professionals must take interim measures to reduce the risk. "You have put the [code in question] behind the firewall or turned off the functionality that's affected," he said.

This issue is gaining attention as Cenzic and Fortify, among application security toolmakers, deliver offerings that look for security flaws in production applications. (Earlier offerings focused more on pre-production applications, written in-house and tested earlier in the development process.)

HARD TO POINT THE FINGER

Commercial software developers aren't held accountable for defects in the same way makers of small appliances, for example, would be. To some extent, that is justified. "Individual software components [licensed from an ISV] may be safe," said Fortify's Chess. "But did you configure them in a secure manner? No software maker can anticipate all the ways code will be used."

What's more, commercial applications, such as those licensed from Oracle or SAP, tend to include vast amounts of customized code, written to connect those applications to the customers' databases and other software, said Jack Danahy, founder and CTO of application security toolmaker Ounce Labs. "So it's hard to point the finger and say the ISV's code is the root cause [of a security flaw]."

Still, commercial software developers should be held to a higher standard, said Gwyn Fisher, CTO of application security toolmaker Klocwork. "We all want products that can't be attacked, and the individuals [writing the software] have to take on the responsibility for that."

Applying pressure on commercial software makers to fix security flaws is a good strategy because it leads to better software. Microsoft would not have worked so hard to address the security flaws in Windows if the problems hadn't been discussed publicly, he said. "That is the beautiful thing about vulnerabilities. People start talking about them, and public advocacy comes to the fore."

Competition works even better, said Caleb Sima, chief technologist of the application security division of HP Software and formerly founder and CTO of SPI Dynamics, acquired by HP last year. The open-source browser Firefox gained traction by positioning itself as more secure than Microsoft's Internet Explorer. "That forced Microsoft to pay attention." In



ComponentArt
Dashboard Development & Core

Let ComponentArt Build Your Dashboard
Built to Your Requirements & Aligned with Your Business Goals



SD Times

Leading the U.S. government to open source
Advocating group seeks to push into federal procurement

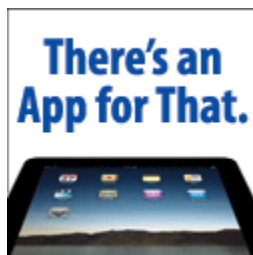
EclipseCan takes up NSA cause
You are looking for... at sports on the Web

Download Current ISSUE 4/15/2010 PDF

Need Back Issues? DOWNLOAD HERE

Receive the print Edition

Subscribe



reality, Firefox is necessarily more secure than Internet Explorer, he added. "What is true is that hackers don't target it as much."

Fortify's Chess said that IT professionals should ask for evidence upfront, before licensing ISV offerings. "Make the vendor prove that security measures have been taken." And if a flaw is uncovered later, expect the software vendor to work with you. "If they don't respond, you can publicly embarrass them," he added. "It's sophomoric, but it's understandable."

Share this link: <http://www.sdtimes.com/link/31695>

Related Articles

[RSA keynote: Lack of security in the cloud breeds distrust](#)

Experts say that until cloud security standards mature and are adopted more widely, adoption will be tepid

[Fortify, HP give hybrid view of app security](#)

By correlating results of dynamic testing and static code analysis, Hybrid 2.0 offers improved vulnerability resolution

[Application security, IBM style](#)

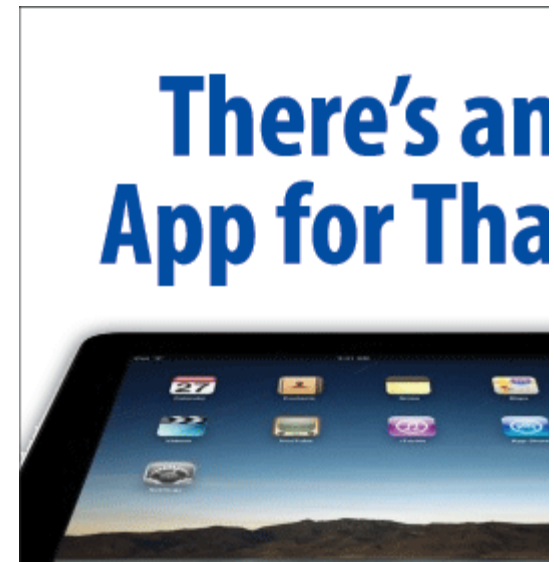
Jack Danahy, founder of Ounce Labs, discusses acquisitions by IBM and what he sees in the security space





Add comment

Name*

Email*

Country



	Alex Handy
	David Rubinstein
	David Worthington
	Katie Serignese

BLOGS

[Invasion of th](#)
 .Doc goes Facet
 ODF goes comm
 does any of this
 matter any more
 04/21/2010 04:54 P

[The lost and i](#)
[iPhone, and a](#)
[ifs](#)
 An Apple engine
 next generation i
 California bar, bu
 seems unscathe
 04/20/2010 04:05 P

[A bevy of link](#)
[impart](#)
 Some links for yc
 pleasure, includi
 nice description i
 machine best pr



[About IDG TechNetwork](#) [Advertise](#) [Become a Member Site](#) [Privacy Policy](#)

[HOME](#) [SITE MAP](#) [CURRENT ISSUE](#) [BACK ISSUES](#) [SUBSCRIBER SERVICES](#) [ABOUT US](#) [CONTACT US](#) [BZ MEDIA](#)

Copyright © 1999-2010 BZ Media LLC, all rights reserved. Legal and Privacy
Phone: +1 (631) 421-4158 • E-mail: info@bzmedia.com