<< Printable version >>

SECURITYFOCUS NEWS

Exploit Code on Trial

By ***Kevin Poulsen***, SecurityFocus Nov 23 2003 9:00PM

Security pros gathering at a Stanford University Law School conference on responsible vulnerability disclosure Saturday harmonized on the principle that vendors should be privately notified of holes in their products, and given at least some time to produce a patch before any public disclosure is made. But there was pronounced disagreement on the question of whether or not researchers should publicly release proof-of-concept code to demonstrate a vulnerability.

UK-based security researcher David Litchfield, of NGS Software, said he publicly swore off the practice after an exploit he released to demonstrate a hole in Microsoft's SQL Server became the template for January's grotesquely virulent Slammer worm. At Saturday's conference, held by the university's Center for Internet and Society, Litchfield said he wrestled with the moral issues for some time. "At the end of the day, part of my stuff, which was intended to educate, did something nefarious, and I don't want to be a part of that," said Litchfield, a prolific bug-finder.

That kind of soul-searching is music to Microsoft's ears. The disclosure standards promulgated by the Organization for Internet Safety, an industry effort founded by Microsoft and handful of large security companies, require researchers to withhold any exploits from the public for at least 30 days following the first public advisory on a bug. But Redmond would like to see researchers abstain entirely, said Steve Lipner, the software-maker's director of security engineering strategy. "We prefer that finders wait before releasing exploit code, or, better, don't release exploit code," he said. "It's something where ... we're trying to ask for cooperation, instead of something that we're trying to mandate or dictate."

California-based security vendor eEye and the Polish white hat hacker group LSD -- both prodigious exploit publishers in the past -- have taken to withholding proof-of-concept code when disclosing serious security holes.

Len Sassaman, security architect at the e-privacy company Anonymizer, says the attitude shift endangers an important part of the Internet's healing cycle when a new vulnerability is discovered. "If the researchers are discouraged from releasing working exploit code... we lose a valuable tool there," he said. "We don't get the proof-of-concept code, we don't get the motivation to create the patch on the vendor side, and to implement it on the user side."

Suppressing exploits also threatens to strip security research of the rigor of serious scientific inquiry, said Matt Blaze, a researcher at AT&T; Laboratories. And network defenders sometimes use proof-of-concept code to evaluate techniques to prevent a compromise, to help detect exploitation of a new vulnerability, and to test that a patch actually works. Conference attendee Warren Stramiello, a network administrator at the Georgia Tech Research Institute, challenged Microsoft's Lipner to come up with a way to do all of that without the help of working code. Lipner countered that exploits aren't very useful to white hats as they're made out to be. "The set of users that would use exploit code to protect themselves... is probably much smaller than the set of people who would be put at risk by it," Lipner said.

Of course, black hat hackers have shown that they're perfectly capable of writing their own exploits. Even the author of the Slammer worm author demonstrated enough skill to have written the worm from scratch, without Litchfield's help. "If anything," said Litchfield,

NEWS

Heckenkamp Challenges Computer Ban
Dec 03, 2003

Nachi worm infected Diebold ATMs
Nov 24, 2003

New charges in Lowe's wi-fi hacks
Nov 21, 2003

Court limits in-car FBI spying
Nov 19, 2003

[archive]

FROM THE WIRES

New computer virus variant floods Web sites of anti-spam activists
Dec 03, 2003

Retail hacker sentenced to 1 1/2 years in prison
Dec 03, 2003

Tech executives try to slow government rules for computer security
Dec 02, 2003

In Norway, appeal of DVD hacker's acquittal begins
Dec 02, 2003

[archive]

"I saved him 20 minutes."

<tips@securityfocus.com>

Discussion

Exploit Code on Trial Anonymous
Screw the vendors Anonymous
  Screw the vendors Rodrigo Otaviano <rodrigo@otaviano.com>
  Screw the vendors? Screw the users at the same time. Alun Jones
Exploit Code on Trial Bob Radvanovsky
Exploit Code on Trial Anonymous
Exploit Code on Trial TW
Private first, then public, THEN publish exploit Anonymous
  Private first, then public, THEN publish exploit Anonymous
Exploit Code on Trial Leif Ericksen
Exploit Code on Trial - final word Anonymous
  Exploit Code on Trial - final word Anonymous
Exploit Code on Trial Camel
Loss of money bl0rf
Exploit Code on Trial Anonymous
Exploit Code on Trial Anonymous
Good on paper....bad in reality. MA

[Post a comment]