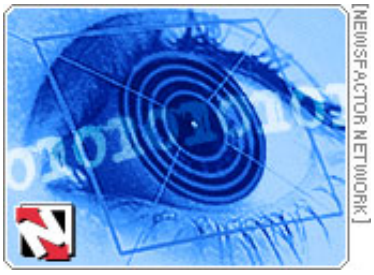
Full Disclosure: How Much Security Info Is Too Much?

By Jay Lyman
www.NewsFactor.com,
Part of the NewsFactor Network
October 2, 2001

Send this Article Related Stories
Print this Article



In publicizing the details of how a given security hole is exploited, are virus fighters simply providing aid and comfort to the enemy?

In This Story:

The debate over how much detail to release on software security gaps and when to go public with potentially sensitive security information has experts looking for a middle ground, wherein systems can be secured without helping hackers.

The Code Red and Code Red II virus outbreaks, which capitalized on vulnerabilities that were publicized before the viruses spread, brought the debate front and center, but the issue presents a constant challenge to those who hunt for vulnerabilities.

Administrators whose systems fell prey to Code Red and Code Red II because they lacked the necessary security patches bore much of the blame for the spread of the viruses. But when considering the bigger picture and the vast numbers of vulnerabilities uncovered every day, the situation becomes more complex, according to CERT vulnerability handling team leader Sean Hernan.

"We are projecting 3,000 new vulnerabilities being publicly announced this year," Hernan told NewsFactor Network. "We try to write clear descriptions with the impact and solution, yet we still get complaints on confusing advisories.

"3,000 vulnerabilities a year -- that's a good chunk of time just trying to evaluate each and every one," he added. "You figure 3,000 times 20 minutes each -- that's 1,000 hours of work, that's half a year of work."

Helping Hackers?

CERT, a center of Internet security expertise at Carnegie Mellon University's Software Engineering Institute, adheres to a 45-day "vulnerability disclosure policy" that puts a hold on security breach information to give software vendors a chance to come up with a patch.

Experts agree that advisories, by their very nature, may be a heads-up to hackers. eEye Security came under fire for disclosing the Code Red vulnerability in June before Microsoft had released a patch for the hole, and again for releasing detailed information after Code Red was controlled, which some blamed for the success of the Code Red II virus.

eEye chief hacking officer Marc Maiffret defended the disclosure, telling NewsFactor that almost all advisories -- whether from individuals or companies -- are irrelevant to hackers.

"It wasn't like we gave a blueprint," Maiffret said. "It doesn't make it easier or harder [for hackers]. A lot of these guys have tools that they can use to find [vulnerabilities] real quickly. They're basically using the same tools we use."

Need To Know

Maiffret claims the majority of security experts support full disclosure.

"It's important for security companies and for researchers to find these [security holes] and have

people support them when they do," Maiffret said.

McAfee Avert senior director Vincent Gullotto, who said that antivirus experts are now working more closely with security experts in response to the crossover between software holes and exploitative computer worms, told NewsFactor that staying updated on security vulnerabilities and patches is as important as updating antivirus software.

Disclosure's Downside

However, Gullotto said there are concerns that some advisories go too far and help those with malicious intent.

"I'm not sure we're in favor of complete and full disclosure," Gullotto told NewsFactor. "To include detail down to the last byte can make it easier for someone to go write a threat."

CERT's Hernan said there are two extremes in the debate, but that to provide an "exploit" or code that demonstrates the security breach along with disclosure of the hole goes beyond what is necessary to secure a system.

"I think that there are many better indicators of whether you're vulnerable," Hernan said. "You don't need to destroy your own system to find out if it's vulnerable."

The Middle Line

There are no rules that govern how much time to give a software vendor to come up with a patch. But Hernan defended large software companies that must take the time to track down the right people and fully investigate security breaches in their products.

However, the vulnerability expert also criticized vendors for shipping products with well-known weaknesses, adding that they should be held more accountable.

CERT's Hernan, who calls the center's 45-day policy a "middle line in terms of time," told NewsFactor that there is also a middle line for how much information is included in an advisory.

"It's not in anybody's best interest to withhold vulnerabilities," he said. "Description and remedial information is important for the public at large, but technical, detailed information is important for security experts. The real nuts-and-bolts probably isn't necessarily useful to the average network administrator." END

See Related Stories

ICANN To Assess Net Address System Security
(01-Oct-01)
Battling Terrorism: Trading Digital Privacy for Nothing?
(28-Sep-01)
Hackers, Spammers May Be Punished as Terrorists
(27-Sep-01)
Chaos: The Coming Technology War
(25-Sep-01)
'War Vote' Virus Can Delete Computer Files
(25-Sep-01)