CERT to disclose software flaws

Robert Lemos, ZDNet News ZDNet.co.uk

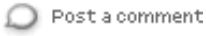
Published: 09 Oct 2000 08:38 BST

- 

- 

- 

- 

- 

It may herald the end of a fight that has inflamed the security community for more than a decade: the Computer Emergency Response Team, or CERT, has endorsed a policy of open flaws in software that could affect security.

The CERT Coordination Centre, which tracks current security threats and publishes advisories to the public, will continue its policy of not publishing any code for exploiting flaws. It will, however, make software security flaws public within 45 days.

The change, announced this week, signals that traditionally conservative organisations are now leaning towards publicly releasing information about software vulnerabilities rather than remaining silent.

The industry "is moving away from polar extremes", said Shawn Hernan, team leader for vulnerability handling for the CERT Coordination Centre, a

part of the Carnegie Mellon University. "There is a philosophy that endorses immediate and complete disclosure and there is a philosophy that endorses complete and utter silence. The trend I see is towards the middle of that."

In the end, the change may mean little difference for CERT members, but increase the pressure on companies to produce better and more secure software.

Three months ago, Marcus Ranum, a well-known security expert and founder of the intrusion-detection software maker Network Flight Recorder, strongly urged a gathering of network professionals to keep secret any security holes found in Internet software and stop creating tools to exploit the holes.

"Full disclosure is creating armies and armies of script kiddies," said Ranum at the Black Hat Security Briefings in July. He went so far as to call the creators of hacking tools "weapons dealers" who aren't really concerned with security. "Distributing [those] tools is not helping," he said.

Yet, while Ranum is well-known in the industry for his black-and-white views on disclosure, most security professionals fall into a grey area.

One such person is Elias Levy, chief technology officer for industry information site SecurityFocus.com. "I think that over the last ten years, full disclosure has moved from an extreme point of view to the accepted point of view," he said.

On its mailing list, SecurityFocus regularly releases information and, sometimes, source code to illustrate the exploit.

"Of all the issues of full disclosure, exploits are the most contentious," he said. While many claim exploits -- source code that illustrate how any

programmer could take advantage of a vulnerability -- only hurt the industry by teaching the enemy, Levy stresses that they are frequently necessary.

"In many cases, they are the best way to explain a problem," he said. "In other cases, an exploit is necessary because a vendor will not try to solve a problem without proof that someone could take advantage of it."

That last behaviour was what another "grey hat" group, known as The L0pht -- who now make up a large part of the research arm of @Stake -- poked fun at on their Web site with this exchange: "'That vulnerability is entirely theoretical.'-- Microsoft L0pht, making the theoretical practical since 1992."

Yet, companies have a legitimate gripe. Media reports abound with security groups that release vulnerability information and exploit code soon after -- or at the same time that -- they notify the flawed software's creator.

A case in point: on Thursday, Bulgarian bug hunter Georgi Guninski publicised a vulnerability in Microsoft's Internet Explorer 5.5 that could allow an attacker the ability to read, write and execute specific files on a PC.

Guninski gave Microsoft only 24 hours before going public with the flaw.

The CERT Coordination Centre hopes its latest move -- in conjunction with talks with some of the major security houses -- will dampen some of the fame-seeking in the industry.

"We are trying to help build an ethos of how to release vulnerability information," said Hernan. "The public has an interest in knowing what the risk is and the vendors have an interest in having enough time." CERT promises to release the name of whoever discovers a bug when they

release their advisory after the 45 day wait.

"This is an attempt to get the community to behave in a rational sort of way," he said.

Take me to Hackers

To have your say *online* click on the TalkBack button and go to the ZDNet News forum.

Let the editors know what you think in the Mailroom. And read what others have said.

Did you find this article useful?
27 out of **70 people** found this useful