Three Minutes with Rain Forest Puppy

Bug hunter crafts full disclosure policy to nudge vendors to acknowledge, fix bugs or be exposed.

Kim Zetter, PCWorld.com
Friday, September 28, 2001

Rain Forest Puppy (RFP) is the handle of a well-known twenty-something hacker and security consultant based in Chicago. In addition to authoring tools that help hackers break into systems, RFP has also discovered a number of security holes in software products, which he has published on the Web after notifying the software maker. He has written a disclosure policy for publishing information about security holes, which serves as a guideline for other bug hunters. *PC World* spoke with him about the protocol for publicizing vulnerabilities and the pros and cons of full disclosure.

PCW: What led you to draft your disclosure policy for publishing software security holes?

RFP: I started looking at the discussions that were going back and forth between vendors and researchers about disclosing bugs. A researcher would disclose a bug without talking to a vendor first, and the vendor would say that the unwritten rule was that the researcher had to tell the vendor first. The term "unwritten rules" kept coming up, and I thought that's the problem, they're unwritten. So I took a stab at writing my own, for my personal use, to get the ball rolling.

PCW: Are you surprised that your policy has become the industry standard?

RFP: I wouldn't say it's an industry standard. A lot of people have taken it and modified it to draft their own. I'm not trying to impose it on other people. I talked to a lot of people in drafting it to get a general consensus, but my way is not necessarily the only way to do this.

PCW: What has been the response from vendors toward your policy?

RFP: Microsoft is for it. They're the only vendor I really got feedback from. I've seen people use it with other vendors, but I haven't really discussed with anyone whether everyone was receptive to that.

PCW: Is the five-day window that you give vendors to respond to a report about a vulnerability appropriate? For instance, in the case of companies that don't have an organized response team set up, it might take them five days just to read your e-mail.

RFP: My policy is that they've got one week, five working days, to return communication. If they don't acknowledge it in a week--if they're on vacation or whatever--then that's already a poor response. Because if you're pushing products out, and you're having security problems, and it takes you a week to even become aware of them, then that's a problem in itself. We're just talking about a matter of initiating communication, not the time in which they need to get the fix out. Some

Related Links

Three Minutes With Microsoft's Scott Culp

Bugs and Fixes: Money Messes From Microsoft, Intuit

MSN Messenger Restored, But Some Buddies Lost

MSN Messenger Mostly Restored

Microsoft Struggles to Restore MSN Messenger

Editors' Picks
Our Top 100 Products:
Select Product Type

Product Finder
Specs & Latest Prices:
Select Product Type

Free Newsletters
Daily Product Review
Daily Best Buy
Enter your e-mail:
Submit
See all newsletters

Instant Alerts
Get email Alerts on stories that match your interest. To choose a keyword, click here.
Keyword Assistant

Expert Help
Need help with your computer question? Choose the right expert at the right price, anytime day or night, at PC World Expert Help.

people do have a policy that says you have seven days to fix this or I'm releasing the announcement. Of course, that's impractical in some situations.

At least, acknowledge [my e-mail], tell me what you're doing to fix the problem. If you need more time, tell me the reasons why you need more time, just explain it to me and be honest. The policy is not about how to disclose the vulnerability, it's more about how to get both parties to effectively open a communication channel and what each one should expect from each other.

PCW: In general, how good are vendors at responding to problems?

RFP: They're getting a little better. The big players at least have become aware of the need to respond and are doing the right thing. The problem is the rapid introduction of new vendors--on a daily basis there are more and more people getting into the game, making software, pushing out products. While one or two vendors start to get it, you have four or five new ones--the mom-and-pop-shops--that haven't encountered this issue yet.

PCW: Is the ratio of holes to lines of code in software getting worse?

RFP: I don't think the ratio is getting worse, the amount of code is increasing. Everyone is doing it bigger and better at such a rapid rate; the code base is just expanding at an enormous rate and because of that bugs are introduced.

PCW: Consumers blame vendors for getting products out too quickly and not putting the effort or money into testing. Is it correct to blame software vendors?

RFP: A company will not sell products if security is its number one focus. Getting the product out to the customer, having it work, and making the money are all first, and security falls down on the list into sixth or seventh place as far as priorities. It really comes down to risk mitigation. If one or two bugs leak through, are they willing to accept that risk? Do they spend extra money and delay the product announcement? If they do, then that affects sales. Unfortunately, that's how business practices are today. It's the push to market attitude: let's just get it out and then we'll go back and fix it later.

But I guess it comes down to who do you blame for a Web-site defacement: the hacker who defaced it, the system administrator who didn't secure his box, or the software vendor because there was a bug in the OS program?

We should really stop looking at trying to point fingers and just get the problem fixed.

PCW: Isn't that what the hacking community is doing, though, laying blame on vendors when they publish a vulnerability announcement and deriding vendors for shoddy products?

RFP: No, we're trying to get the bugs fixed. If the vendor is responsible and we can open up a communication channel, then we succeed at that.

PCW: You sometimes work closely with Microsoft to help them find and fix holes in their products. What is your relationship with the company?

RFP: When I find a vulnerability, I'll follow my policy with them. As long as they're receptive and keep communication open and keep me in loop, I'll work with them.

PCW: When was the last time you found a bug in one of their products?

RFP: That would be the Unicode bug which I found last December. They were immediately responsive. I mailed them at around 2 a.m. on a Friday night and got a response from them a couple of minutes later. They had a patch turned around in two days.

PCW: Which other software vendors do you work with?

RFP: A lot of smaller vendors which tend to be free software vendors. I really try to help them out on a personal level because it's typically a hobby product [of the maker]. Some of them are responsive and some of them aren't. I try to take the time to explain why they should be receptive and to explain the problem. Here are some patches that they should apply [to their product] and why.

PCW: Are software vendors lazy when it comes to testing their products?

RFP: They don't take the time to find problems. The historical record is great right now with information about vulnerabilities. And if a vendor, before making product xyz, would go to the historical security record and look at other products that are similar to xyz and see what bugs those products had and double-check to make sure

that their product doesn't have them, I think a lot of the vulnerabilities would be reduced.

Printer Friendly Version