antiSecurity

save a bug, save a life

choose language: [en],ru,fr,de

Menu

Main
News
FAQ
Texts
Board
Gallery
Links

Contact us with email:
anti@security.is

visits: 5908

Intro

The purpose of this movement is to encourage a new policy of anti-disclosure among the computer and network security communities. The goal is not to ultimately discourage the publication of all security-related news and developments, but rather, to stop the disclosure of all unknown or non-public exploits and vulnerabilities. In essence, this would put a stop to the publication of all private materials that could allow script kiddies from compromising systems via unknown methods.

The open-source movement has been an invaluable tool in the computer world, and we are all indebted to it. Open-source is a wonderful concept which should and will exist forever, as educational, scientific, and end-user software should be free and available to everybody.

Exploits, on the other hand, do not fall into this broad category. Just like munitions, which span from cryptographic algorithms to hand guns to missiles, and may not be spread without the control of export restrictions, exploits should not be released to a mass public of millions of Internet users. A digital holocaust occurs each time an exploit appears on Bugtraq, and kids across the world download it and target unprepared system administrators. Quite frankly, the integrity of systems world wide will be ensured to a much greater extent when exploits are kept private, and not published.

A common misconception is that if groups or individuals keep exploits and security secrets to themselves, they will become the dominators of the "illegal scene", as countless insecure systems will be solely at their mercy. This is far from the truth. Forums for information trade, such as Bugtraq, Packetstorm, www.hack.co.za, and vuln-dev have done much more to harm the underground and net than they have done to help them.

What casual browsers of these sites and mailing lists fail to realize is that some of the more prominent groups do not publish their findings immediately, but only as a last resort in the case that their code is leaked or has become obsolete. This is why production dates in header files often precede release dates by a matter of months or even years.

Another false conclusion by the same manner is that if these groups haven't released anything in a matter of months, it must be because they haven't found anything new. The regular reader must be made aware of these things.

We are not trying to discourage exploit development or source auditing. We are merely trying to stop the results of these efforts from seeing the light. Please join us if you would like to see a stop to the commercialization, media, and general abuse of infosec.

Thank you.