Microsoft Reveals Anti-Disclosure Plan

Five computer security firms join Microsoft to set an official standard for limiting disclosure of software security holes

Kevin Poulsen Nov 9 2001 2:04AM PT

NEWS

MOUNTAIN VIEW, Calif.--Microsoft and five major computer security companies rounded up the three-day Trusted Computing Forum on Thursday by formally announcing a coalition against full disclosure of computer vulnerability information, ending a week of intense speculation, and immediately sparking controversy.

Bindview, Foundstone, Guardent, @Stake, and Internet Security Systems joined with the software-maker to declare they would immediately begin following a policy of limited public disclosure of security vulnerability information. Members of the coalition who discover new vulnerabilities will omit from their initial public advisories any details about how a hole might be exploited in an attack, and will not include code that demonstrates the bug. Thirty days after the first advisory, a more detailed noticed can be released under the rules.

"We felt that as responsible industry leaders, we, as a voluntary

organization, are going to follow a set of reasonable standards," said Scott Culp, manager of Microsoft's security response center, in an interview.

The still-unnamed organization will also draft a proposed international standard for notifying vendors and the public about newly-discovered software security bugs, following the group's limited disclosure ethic. The organization will admit new members, under an as-yet unwritten set of bylaws.

A chief objective of the group is to discourage 'full disclosure,' the common practice of revealing complete details about security holes, even if publication might aide attackers in exploiting them.

Publishing complete information, and sometimes "exploit" code that demonstrates a vulnerability, is *de rigueur* among many computer security professionals, who argue that malicious hackers can acquire the same information themselves, and that network administrators and security gurus often need technical details to properly defend themselves from attack.

'If it becomes hard to release vulnerabilities, that's a good way for Microsoft to get rid of some embarrassment.'
-- Marc Maiffret,

But Culp criticized the practice in an essay published on a Microsoft Web site last month, and blamed "information anarchy" for the epidemic of malicious worms that have struck the Internet in the last year. "It's high time the security community stopped providing blueprints for building these weapons," Culp wrote.

Internet Standards Approach

The new organization's plan has two parts. In the months ahead, coalition members will produce a set of RFCs, 'Requests for Comments,' that will set out

eEye Digital Security

procedures for handling new security holes. The proposals would cover every aspect of security bug reporting, including the form of reports and advisories, standard email contacts for vendors to receive bug reports, and timetables for vendor response and limited public disclosure.

The RFCs will be submitted to the Internet Engineering Task Force, the Internet's technical standard-setting body, where it will be open to public review and comment, and considered for adoption as an official standard.

If the proposal becomes an approved Internet standard, proponents say they'll use it to pressure security researchers to go along. "We've seen in other situations that pressure come to bear," says Eddie Schwartz, senior vice president and COO for Guardent.

The group's second tactic is to lead by example. "In the short term, there are going to be bylaws for this organization," says Chris Wysopal, director of research and development for @Stake, and the chief architect of the plan.

Members of the organization will commit to a 30-day "grace period" in which only vague information about a vulnerability is made public. The bylaws will also include an agreement that any security software produced by members of the group will be engineered in such a way that it can only be used for lawful purposes.

Wysopal's leadership role in the group may lend it added cachet, or at least a touch of irony. Until recently, Wysopal answered to the hacker handle "Weld Pond," a vestige of his days as a member of the white hat hacker collective the L0pht. Prior to becoming @Stake's founding research team, the L0pht was famously supportive of full disclosure, and created the password-cracking tool L0phtCrack -- used by security

professionals and intruders alike.

'Information Cartel'

But even before Thursday's announcement, the notion of limiting disclose of security information was controversial, and critics were not appeased by the added details.

"What's being created here is an information cartel," says Elias Levy, former moderator of the Bugtraq security mailing list, a standard outlet for 'full disclosure' security information. "It actually benefits security vendors to have limited vulnerability information, because it makes them look better in the eyes of their customers," says Levy. (Levy is CTO of SecurityFocus).

Under the plan, member companies would share detailed information during the 30-day grace period with law enforcement agencies, infrastructure protection organizations, and "other communities in which enforceable frameworks exist to deter onward uncontrolled distribution." The last category would allow member companies to share details with clients under a non-disclosure agreement, and to share details with one another. "They're not going to ban it among themselves," says Levy. "They might be willing to limit the public access to this information, but I highly doubt that they'll limit it among each other."

Marc Maiffret, co-founder of eEye Digital Security, agrees, and charges that the coalition was formed for the commercial advantage of its members, rather than the well-being of the Internet.

"If it becomes hard to release vulnerabilities, that's a good way for Microsoft to get rid of some embarrassment," says Maiffret.

Maiffret's company is responsible for discovering some of the most

serious Microsoft security holes in recent years -- vulnerabilities in the company's IIS web server product that allow attackers to gain remote control of the system. He says eEye cooperates with vendors, and doesn't release advisories until a company has had a chance to produce patches for the security hole. But Maiffret rejects the idea of holding back on technical details, and warns that the new coalition may alienate independent security researchers.

"People have to do it Microsoft's way or they'll have this group telling them that they're acting irresponsibly," says Maiffret. "It's going to drive people into the underground, and could lead to more people breaking into computers."

"It's not trying to form a secret society of exploits," says Christopher Klaus, founder and CTO of Internet Security Systems, a backer of the proposal. "It's just creating a standard... This represents one of the first process standards between security companies and vendors."

Wysopal estimates it will take one or two months to produce drafts of the proposed RFCs. He emphasizes that the standards would not just limit vulnerability disclosure, but would also spur vendors to be more responsive to security vulnerability reports. "My goal in the RFC is to have equally stringent standards for vendors as researchers," says Wysopal.

Discussion
Microsoft Reveals Anti-Disclosure Plan *Anonymous*
Microsoft Reveals Anti-Disclosure Plan *Anonymous*
What about the admins? *ferretzero*
Microsoft Reveals Anti-Disclosure Plan *Anonymous*
Microsoft Reveals Anti-Disclosure Plan *russell handorf*

Microsoft Reveals Anti-Disclosure Plan *Angus Blitter*
30 days makes no difference *Anonymous*
Microsoft Reveals Anti-Disclosure Plan *Anonymous*
Microsoft Reveals Anti-Disclosure Plan *Bill Gaytes*
Microsoft Reveals Anti-Disclosure Plan *I am Stunned*
Microsoft Reveals Anti-Disclosure Plan *Anonymous*
Microsoft Reveals Anti-Disclosure Plan *kishg@optonline.com*
Microsoft Reveals Anti-Disclosure Plan *Anonymous*
Shocking developments *H Carvey <keydet89@yahoo.com>*
Shocking developments *Anonymous*
Shocking developments *Greggory Peck*
Microsoft Reveals Anti-Disclosure Plan *Steve*
l0pht like the other members has sold his soul. *Anonymous*
MS knows exactly what they're doing. *Anonymous*
Microsoft Reveals Anti-Disclosure Plan *Tommy Ward*
Download Utilities now, while you can *anonymous*
Be careful what you wish for. *Surreal*
Microsoft Reveals Anti-Disclosure Plan *nogrhi*
Microsoft Reveals Anti-Disclosure Plan *Big Bangular*
Such a policy for disclosure already exists *Dumky*
Such a policy for disclosure already exists *H Carvey <keydet89@yahoo.com>*
Microsoft Reveals Anti-Disclosure Plan *Anonymous*
Microsoft Reveals Anti-Disclosure Plan *Anonymous*
Microsoft Reveals Anti-Disclosure Plan *Anonymous*
Microsoft Reveals Anti-Disclosure Plan *Anonymous*
Microsoft Reveals Anti-Disclosure Plan *Anonymous*
Re:Microsoft Reveals Anti-Disclosure Plan *Uhh*
...on second thought...Kudos! *H Carvey <keydet89@yahoo.com>*
RE: ...on second thought...Kudos! *Gregarious Monk*
Microsoft Reveals Anti-Disclosure Plan *Anonymous*

Microsoft Reveals Anti-Disclosure Plan *Anonymous*
RFP (Rain Forest Puppy) *Anonymous*
Microsoft Reveals Anti-Disclosure Plan *Anonymous*
microsoft TERRIBLE SOFTWARE anyway *Anonymous*
Managed Security Services Industry? *Dogsend*
Microsoft Reveals Anti-Disclosure Plan *Anonymous*
So what would force Microsoft to patch these holes if exploits are not published? *Rafal Sybilla-Leszczynski*
[Post a comment]