World Socialist Web Site wsws.org

Serious security flaws in Microsoft web browser

How safe is your computer?

Mike Ingram
12 January 2002

If you are using an operating systems from Microsoft, the answer to the question, “how safe is your computer?” would have to be “not very!”

The software giant at the centre of a number of antitrust cases in the US and now Europe is proving itself increasingly incapable of protecting the basic security of its customers. Despite the release of the new Windows XP operating system, which introduces many security features not available in earlier operating systems such as Windows 98 and 95, users still face a continuous barrage of virus alerts and notices of security holes.

Most recently, an independent researcher going by the name of “ThePull”, accused Microsoft of a serious security breach by ignoring a security rule knows as the “same origin policy”. This rule is designed to prevent code from one website affecting another site opened in a different window of a web browser.

JavaScript is a widely used scripting language that can automate many actions such as printing or saving a web page, etc. It includes the command “document.open,” which allows a second browser window to be opened in response to certain user actions. This command is commonly used to open a second window containing a print version of a particular file. Sites also frequently use the command to open new windows containing advertisements or other information.

Developed as part of the JavaScript security guide written by engineers at Netscape (who produced the first widely used web browser), the “same origin policy” was established to prevent malicious websites from interacting with and taking sensitive information from other sites opened in different windows by the browser.

“ThePull” alleges that Microsoft has ignored this policy and that versions 5.5 to 6.0 of its popular Internet Explorer browser permit such operations. This could allow an attacker to set up a specially constructed website capable of stealing information from a viewer’s cookie files. Cookies are locally stored files used by websites to identify users on repeat visits. Popular with E-commerce sites, cookies can contain anything from user IDs and passwords, to credit card numbers. As well as the possible theft of personal information contained in cookies, the security flaw could also be used for “spoofing”—fooling a visitor into believing they are visiting a trusted, legitimate site, one which they may submit personal data to, such as an online bank, for example.

Such an exploit was reported publicly on November 8, causing Microsoft to issue a security notice the same day advising customers to disable “Active Scripting,” which would protect them from web-hosted and mail-borne variants of the vulnerability, though hindering users in their ability to browse certain sites.

Microsoft’s initial response to the news of this security flaw was to accuse the firm that had revealed it of “irresponsibility”. Microsoft claimed to know nothing of the security hole prior to the November 8 notice. According to an article on the ZDNet UK technology site November 19, however, the company later admitted it was actually notified of the bug a week earlier on November 1.

Microsoft claimed that two whole weeks were needed to investigate the alert properly, and insists that no security breaches occurred as a result of the delay.

“We are obviously not going to respond instantly—we have to sieve the wheat from the chaff to determine how reliable the vulnerability warning is,” Windows product marketing manager Neil Laver told ZDNet. “Until we can investigate the issue, we are not going to issue a bulletin, as that would create a crying wolf situation.”

But ZDNet reports that Microsoft not only failed to issue a public notice on the vulnerability, it also failed to provide any feedback to those who had notified it of the security hole.

IT security firm Online Solutions supplied Microsoft’s Security Response Centre with technical details of its discovery of a serious security breach on November 1. Microsoft acknowledged the alert and promised that it would investigate the issue as quickly as possible. After one week, and no feedback from Microsoft, Online Solutions decided to go public.

"We did the responsible thing—people who are using software that their business relies on to hold personal information, should be aware in reasonable time that the program is not secure," Jyrki Salmi, managing director of Online Solutions said.

Security holes are by no means limited to Microsoft software. Containing millions of lines of computer code, complicated applications such as Internet Explorer are notorious for bugs, not all of which are ironed out in the beta testing stage. A large part of a computer systems administrator's job consists of applying patches to software in response to security announcements for the myriad of applications and utilities running in any system. To the extent that those developing the software respond quickly, and issue fixes as soon as possible, most potential security holes should not cause serious problems. The issue with Microsoft is not that its programmes have holes in them, but that it fails to issue patches within an acceptable time and does not disclose known vulnerabilities to users of its software, even when a simple work-around is available—as with disabling Active Scripting in the most recent cases.

Microsoft claims that if it had issued such a notice, this may have alerted malicious hackers to the vulnerability and compromised user security further. A more plausible explanation is that the company hoped to quietly release a fix and avoid any adverse publicity.

As the US courts try to find ways to make Microsoft pay for its antitrust violations, and nine of the original states involved in the lawsuit continue to reject the proposed settlement, the company's security failures will undoubtedly fuel regrets that the software giant was not broken up, as proposed by Judge Jackson.

The original trial heard how Microsoft had used its monopoly in desktop operating systems to gain a market lead for its Internet Explorer web browser. Microsoft was concerned to prevent the rival Netscape browser, which had a far wider user base initially, from becoming an alternative platform to Windows for developing applications. In the course of the trial, Microsoft insisted that Internet Explorer had won out because it was a better product than Netscape Navigator. In fact, Microsoft had been caught out by the rapid popularity of the World Wide Web, and rushed out Internet Explorer, which it gave away free, in an effort to win ground back from Netscape.

The ultimate rejection of Judge Jackson's proposals led to calls for other restrictions on Microsoft and demands that the Internet Explorer source code—which defines the essential functioning of a programme—be made available.

Microsoft initially sought to rationalise its monopoly position by arguing that the wide use of its products was simply because they offered technical superiority. However, the rise of "Open Source software," and particularly programmes running on the freely available Linux operating system, has produced a change in tack by Microsoft. According to *Guardian Online*, "It has abandoned its arguments based on technology, and turned, with what looks increasingly like desperation, to the area of intellectual property."

The paper cites Microsoft CEO Steve Ballmer saying, "Linux is a cancer that attaches itself in an intellectual property sense to everything it touches."

Whereas Microsoft claims that Open Source is simply about people wanting something for nothing—free software—in reality, its advocates are rarely motivated by the question of cost. Their central concern is that software users should have free access to the source code, so that it can be altered to give programmes greater functionality and other improvements made as required.

Microsoft now faces antitrust investigation by the European Commission, the executive arm of the European Union. The EC is investigating whether the software giant has used its market dominance in desktop operating systems to unfairly gain a share in the server market. A ruling in the case is expected some time in the next few months. The EC has the power to impose fines of up to 10 percent of the Microsoft's revenues, equivalent to $2.5 billion.

Whatever action the EC takes, as with the US case, it will do nothing to address the interests of the millions of ordinary people throughout the world for whom computers form an increasingly important part of their daily lives. Inevitably, the notion of Open Source comes into direct conflict with a social system based upon the accumulation of private profit, and dominated by massive transnational corporations such as Microsoft.