

TECH

Pregnant pause OK for Microsoft

Patrick Gray
July 17, 2007
Next



Security experts say Microsoft was justified in taking nine months to patch a serious security hole in its .NET framework, discovered last October. Security-Assessment.com penetration tester Paul Craig, who uncovered the vulnerability, says Microsoft did the right thing by applying time-consuming regression tests to the fixes it released last week.

Regression tests check whether a fix to one problem has created new problems. .NET is a library of software "spare parts" used to create web and Windows applications.

"Microsoft goes through quite a large (quality assurance) process," Mr Craig says. "I think Microsoft does a pretty good job of testing its applications . . . I would be more shocked if they put out a patch in a week."

Fixes for several flaws in Microsoft's .NET framework were released last week, the most serious of which allowed remote attackers to seize control of computers running the Microsoft software. The flaw uncovered by Mr Craig would have allowed attackers to read web-server configuration and source-code files, potentially revealing sensitive information such as database credentials or encryption keys, he says. "There (were) logic flaws within .NET itself, with the language interpreter."

Adam Pointon, a security consultant with assurance.com.au, agrees the time taken to develop the patch was reasonable, given how ingrained the .NET framework is in all recent Microsoft operating systems and applications.

The level of regression testing the company needed to perform to ensure the patch didn't "break" customer configurations would have been daunting, Mr Pointon adds.

"If it was a buffer overflow in some crappy (network service), then sure, it should be fixed in seven days. But because it's so core I don't blame them for taking so long," he says.

In the past, Microsoft has been criticised for taking too long to fix vulnerabilities.

Via email, Microsoft Security Response Centre director Mark Miller says all security patches go through a rigorous testing process. "Experts investigate the scope and impact of a threat on the affected product," he says. "Once the update is built, it must be tested with the different operating systems and applications it affects, then localised for many markets and languages across the globe."

However, users reported problems with the patch in online forums over the weekend, and Microsoft has documented nine problems with the update.

More bugs in the .NET framework may follow Mr Craig's discovery of the so-called Null Byte Termination Vulnerability. "The immediate instances of the vulnerabilities that I found were fixed by the patch . . . but other parts of the framework could still be vulnerable," he says. "(This is) a new class of attack, it's a new way of attacking .NET applications."

More of Patrick Gray's interview with Paul Craig can be heard in his podcast from ITRadio.com.au/security

Advertisement

Research Matters
Experience Research Excellence
16 - 27 August 2010

MONASH University
CRICOS Provider Number: 00008C

Advertisement