PHYS.ORG

Microsoft offering defenses against Duqu virus

November 4 2011

The Microsoft logo is seen in June 2011 in Los Angeles, California. Microsoft on Friday was advising companies how to defend against infection by a Stuxnet-like Duqu virus.

Microsoft on Friday was advising companies how to defend against infection by a Stuxnet-like Duqu virus.

The US technology colossus released the "workaround" along with detailed information it said would enable anti-virus software companies to detect Duqu, which takes advantage of a flaw in Windows computer operating systems.

"To make it easy for customers, we have released a fix-it that will allow one-click installation of the workaround and an easy way for enterprises to deploy," said Microsoft trustworthy computing group manager Jerry Bryant.

"Our engineering teams determined the root cause of this vulnerability, and we are working to produce a high-quality security update to address it," he said in a security advisory posted online.

A software patch to protect against Duqu will not be ready in time for this month's "update Tuesday" next week, according to Microsoft.

Duqu can sneak into computers by hiding in Word document files opened as email attachments.

Duqu infections have been reported in a dozen countries including Iran, France, Britain and India, according to US computer security firm Symantec.

The virus takes advantage of a previously unknown vulnerability in a Windows font-parsing engine to plant malicious code in the heart of a computer system, according to Microsoft.

"An attacker who successfully exploited this vulnerability... could then install programs; view, change, or delete data; or create new accounts with full user rights," Microsoft warned in a security advisory.

"We are aware of targeted attacks that try to use the reported vulnerability; overall, we see low customer impact at this time," it said.

Stuxnet was designed to attack computer control systems made by

German industrial giant Siemens and commonly used to manage water supplies, oil rigs, power plants and other critical infrastructure.

Most Stuxnet infections have been discovered in Iran, giving rise to speculation it was intended to sabotage nuclear facilities there

Citation: Microsoft offering defenses against Duqu virus (2011, November 4) retrieved 9 April 2024 from https://phys.org/news/2011-11-microsoft-defenses-duqu-virus.html