

Microsoft Plugs IE; Report Warns All Browsers At Risk

Source: <http://sci.tech-archive.net/Archive/sci.med.transcription/2004-07/0313.html>

From: leslie (*LESLIE_at_JRLVAX.HOUSTON.RR.COM*)

Date: 07/03/04

Date: Sat, 03 Jul 2004 21:53:00 GMT

<http://www.securitypipeline.com/news/22103560>

Security Pipeline | News |

Microsoft Plugs IE; Report Warns All Browsers At Risk

"July 02, 2004

Microsoft Plugs IE; Report Warns All Browsers At Risk

By Gregg Keizer Courtesy of TechWeb News

As if to prove the point that security is like the Dutch boy at the dike, Microsoft on Friday released a stop-gap fix for one of several vulnerabilities that have plagued its Internet Explorer just as a security firm warned that virtually every browser -- not just IE -- can be spoofed by hackers.

The update, which Microsoft tagged as "Critical," isn't a patch per se, but rather an change to Windows that disables the ADODB.Stream object within the operating system's Data Access Components (DAC).

Last week, an innovative attack launched by a Russian hacker group from previously-infected Microsoft Internet Information Services (IIS) servers compromised a large number of PCs with identity- and financial information-thieving Trojan horses and key loggers. The attack exploited a pair of vulnerabilities in Internet Explorer, one of which -- ADODB -- had not been patched by Microsoft.

While the Russian Web site that hosted the malicious code -- which was surreptitiously downloaded to the compromised computers -- was taken down last Friday to remove the immediate danger, Microsoft has still not released a patch. The ADODB disabler is meant only as a temporary fix, said Microsoft, until it can permanently fix IE.

"In addition to this configuration change, Microsoft is working to provide a series of security updates to Internet Explorer in coming weeks that will provide additional protections," said Microsoft in a

statement. Microsoft did not offer up a timeline for any future IE patches, saying only that "a comprehensive update will be released once it has been thoroughly tested."

The update to disable ADODB should be downloaded and installed by all users of Windows NT, Windows 2000, Windows XP, and Windows Server 2003, Microsoft said. It's available on the Windows Download site, or via the Windows Update service. Windows XP Service Pack 2 (SP2), which is expected to release in final form this summer, is not susceptible to the ADODB vulnerability.

Friday's update is one of the few pieces of good news IE users have heard in the last week.

After a rash of exploits against IE vulnerabilities -- including the Web attack of last week, password-stealing Trojans, and a new way for hackers to spoof, or fake, Web sites -- some security analysts questioned whether Internet Explorer was safe enough to use.

Even the U.S. Computer Emergency Response Team (US-CERT), part of the federal government's Department of Homeland Security, recommended that users consider ditching IE for an alternate such as Mozilla or Opera.

"We're recommending one of two things," said Thomas Kristensen, the chief technology officer at Danish security firm Secunia. "Either use Internet Explorer under very restricted security settings -- which may not be possible for all companies -- or install a different browser."

Wednesday, Secunia issued a warning saying it had discovered a vulnerability within IE that allowed scammers to spoof, or fake, the content of a site displayed in the browser.

On Friday, however, the security vendor modified the alert to claim that virtually every browser, from Internet Explorer and Mozilla to Opera and Netscape -- including browsers for both Windows and the Mac OS -- has this flaw.

"It's not a code vulnerability," said Secunia's Kristensen, "but a design flaw."

The problem stems from how browsers handle frames. "Some time ago, browser designers decided that one site needed to be able to manipulate the content of another, and the functionality was adopted by everyone," said Kristensen. But hackers can use this to inject phony content -- say their own credit card-stealing form -- into a frame of an actual trusted Web site, such as a user's online bank.

"In these times of phishing attacks and other scams, this is a problem," said Kristensen. "You're visiting a bank or an e-commerce site, and you're certain of that site, but meanwhile, it's [actually] open in the background to content change by hackers."

sci.med.transcription: Microsoft Plugs IE; Report Warns All Browsers At Risk

Internet Explorer users can stymie such spoofing attacks by disabling the "Navigate sub-frames across different domains" setting under Tools/Internet Options/Security.

Secunia offered up a quick test that users can run to see if their current browser is vulnerable to this problem."

The "quick test" link points to a page for testing the vulnerability in question:

http://secunia.com/multiple_browsers_frame_injection_vulnerability_test/

Jerry