CSO

NEWS

Microsoft patches yet another Hacking Team zero-day exploit

The vulnerability was located in the Windows Media Center software

By Lucian Constantin | Follow
IDG News Service | Sep 9, 2015 3:06 PM PT

Over two months after Italian surveillance software maker Hacking Team had its internal data leaked by hackers, vendors are apparently still fixing zero-day exploits from the company's arsenal.

On Tuesday, Microsoft published 12 security bulletins covering 56 vulnerabilities in the new Edge browser, Internet Explorer, Windows, Office, Skype for Business, .NET Framework and some of its other software products.

One of those vulnerabilities, identified as CVE-2015-2509, was located in the Windows Media Center and had zero-day status -- it was publicly disclosed before the patch was released.

In the accompanying security bulletin Microsoft says that despite the public disclosure, the company "had not received any information to indicate that this vulnerability had been publicly used to attack customers."

However, a working and reliable exploit for it was found in the leaked Hacking Team data and the company ran a service through which it shared zero-day exploits with its customers for use in the deployment of surveillance software.

In July, security researchers searching through the leaked Hacking Team files found exploits for six zero-day vulnerabilities: three in Flash Player, two in Windows and one in Internet Explorer. Some of those exploits were quickly adopted by various groups of attackers after being leaked.

According to security researchers from Trend Micro, who reported the newly patched Windows Media Center vulnerability to Microsoft, an exploit for it was found in Hacking Team's data.

Based on a description found in the company's leaked emails, the exploit was quite recent because it had been tested against Windows Media Center running on Windows 8.1, 8 and 7 with the April 2015 security updates installed.

The exploit consists of a specifically crafted Media Center link (.mcl) file and could be delivered to targeted users in different ways including as a download from a website, by e-mail or via instant messaging applications, the Trend Micro researchers said in a blog post Tuesday.

Creating malicious .mcl files that would exploit this vulnerability can easily be done using a text editor like Notepad, they said. "For example, we created a .MCL file that contained instructions that will launch the computer's calculator."

Since information about the exploit has been available on the Internet for over a month, due to the Hacking Team leak, cybercriminals might start using it in attacks, the Trend Micro researchers said. "We recommend users avoid opening any files with the .MCL file extension, especially from unverified sources."

Lucian Constantin — *Romania Correspondent*

Insider: How a good CSO confronts inevitable bad news ›

View Comments

How Do Pro Golfers Swing So Fast?

Revolution Golf

10 Website Builders That Really Work

Top 10 Website Builders

VMware's virtual approach to containers

10 security technologies destined for the dustbin

Blackmail rising from Ashley Madison breach

Quick Reference Guide for Intel® Core™ Processor Graphics | Intel® Developer Zone

Intel