Security

Redmond yells 'CUT' on Hacking Team horror movie exploit

Media Player attack closed off

10 Sep 2015 at 06:30, Darren Pauli 48 8

Another of exploits against Microsoft Windows that hit as a zero day after Hacking Team was hacked has been fixed.

Trend Micro threat bod Kenney Lu says the fix for CVE-2015-2509 was among the 56 of this week's Patch Tuesday bug-splat.

Hacking Team's remote code execution exploit works on Windows Vista through to 8 and works if a victim opens a crafted Media Center link file which contains malcode.

Lu says the exploit works 'perfectly' on Windows Media Centre.

"This vulnerability is related to a previously unreported zero-day exploit discovered in the Hacking Team leaked emails," Lu says.

"Trend Micro researchers discovered the exploit and subsequently reported their findings to Microsoft.

"Based on information in the emails, the exploit works perfectly with the latest version of Windows Media Center."

It grants attackers the same user rights as the current user meaning those users with reduced access privileges will be of less value to bad guys.

Attackers can send the corrupt file through their vector of choice including email or drive-by-download Lu says.

A user need only open the file to be p0wned.

While Redmond says there is no indication net scum are targeting CVE-2015-2509 it is highly likely they will since the Hacking Team exploits have been publicly available for weeks.

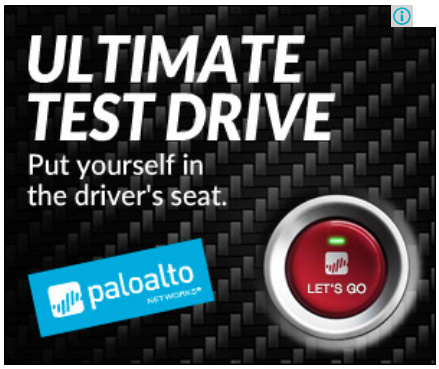
Indeed Lu expects crims to jump on the bandwagon as is common after a big patch run.

Users should steer clear of ~~all~~ Media Centre link files until patches are applied as there are no

More like this

Vulnerabilities Exploits

Security Patching



Most read


Wileyfox Swift: Brit startup budget 'droid is the mutt's nuts


Russian regulator bans PornHub for its 'illegal pornography'


Laminate this: Inside Argos' ongoing online (r)evolution


It's still 2015, and your Windows PC can still be pwned by a webpage


Well, what d'you know: Raising e-book prices doesn't raise sales

Spotlight


Attention sysadmins! Here's how to dodge bullets in a post-Ashley Madison world

mitigations or work arounds. ®

Tips and corrections

Post a comment

More from The Register

Fragmented Android development creating greater security risks

Some flaws exist on over a ‘hundred phone models and affect millions of users’

22 Comments

DeathRing: Cheapo Androids pre-pwned with mobile malware

Ringtone app's crap, dangerous and impossible to remove

8 Comments

Windows and OS X are malware, claims Richard Stallman

'Resist gratification', says super-GNU-man freedom fighter

201 Comments

You shouldn't be paying for mobile ads (please buy our software)

Ad-blocking company selflessly campaigns for the blocking of ads

16 Comments

Brit school software biz unchains lawyers after crappy security exposed

Bug hunter went full-disclosure with baked-in encryption key

72 Comments

Nasty Dyre malware bests white hat sandboxes

Core checker a defensive wrecker

11 Comments

Whitepapers

The seven stages of advanced threats

Gain a deeper understanding of the seven stages of advanced threats and how they affect your organization

Mitigating risks with security intelligence and identity assurance

Describing how intelligent IAM solutions help defend against insider threats, manage access and boost compliance

VersaStack for data center with direct attached storage

Describing the architecture and deployment procedures of an infrastructure composed of Cisco, IBM, and VMware virtualization.

IBM: The optimal storage platform for big data

The landscape of data required for analytics is evolving rapidly. In this white paper learn about the important requirements that you should consider.

Viral virus bunfight: Dr Web tested rivals like Kaspersky Lab

Prepare to be Thunderstruck: What if 'deuszu' ISN'T the Ashley Madison hacker?

Malware menaces poison ads as Google, Yahoo! look away

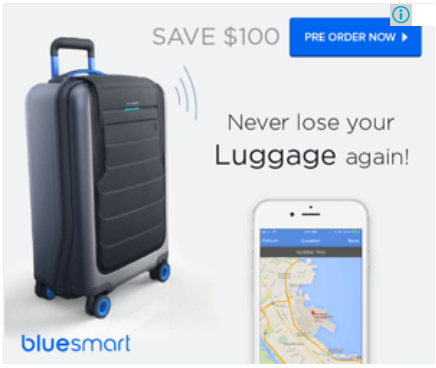
Carders fleece $4.2 million from Victoria's MyKi transport agency

Telstra News spews banking trojan after malvertising attack

Want security? Next-gen startups show how old practices don't cut it

Rise up against Oracle class stupidity and join the infosec strike

Patching a fragmented, Stagefrightened Android isn't easy



Sponsored links

Sign up to The Register to receive newsletters and alerts

The Register
Biting the hand that feeds IT © 1998–2015
Independent news, views, opinions and

reviews on the latest in the IT industry. Offices in London, Edinburgh, San Francisco and Sydney.