MUST READ Microsoft fixed the Windows Media Center Hacking Team bug with the

Microsoft fixed the Windows Media Center Hacking Team

This month's Patch Tuesday features 12 updates including a fix for a Windows Media Center Hacking Team exploits reported to Microsoft by Trend Micro.

In June, the Italian surveillance firm Hacking Team suffered a dramatic data breach, attackers

leaked internal data of the company, including email messages and source code of the zero-day exploits used by the firm. This week Microsoft published 12 security bulletins related to 56 vulnerabilities affecting a number of products including the new Edge browser, Internet Explorer, Windows, Office, Skype for Business, .NET Framework and some of its other software products.

Among the fixed vulnerabilities, there is also the CVE-2015-2509 that affected the Windows Mec Center and could allow to gain the same user rights as the current user on the target machine.

"The vulnerability could allow remote code execution if Windows Media Center opens a speciali crafted Media Center link (.mcl) file that references malicious code. An attacker who successfull exploited this vulnerability could gain the same user rights as the current user. Customers who accounts are configured to have fewer user rights on the system could be less impacted than th who operate with administrative user rights."

states the Microsoft security bulletin.

Microsoft also added that despite the public disclosure of the zero-day, it "*had not received any information to indicate that this vulnerability had been publicly used to attack customers.*"

However, the Hacking Team's dump includes a working exploit for this flaw that is included in th surveillance software commercialized by the Italian firm.

Following the disclosure online of the Hacking Team Dump, security firms discovered the code t three zero-day in Flash Player, two in Windows and one in Internet Explorer. APTs groups and criminal crews immediately started adopting them in their campaigns.

According to experts at Trend Micro, who uncovered the Windows Media Center vulnerability fi

The exploit appears quite recent because according to an internal email of the surveillance firms, it had been tested against Windows Media Center running on Windows 8.1, 8 and 7 with the April 2015 security updates installed.

"One of the important updates addresses a vulnerability found in the Windows Media Center (CVE-2015-2509). This vulnerability is related to a previously unreported zero-day exploit discovered in the Hacking Team leaked emails. 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." states a blog post published by Trend Micro.

4. Affected OS
[X] Windows 8 64 Patch level ___ Windows 8.1 with April 2015 updates
[X] Windows 8 32 Patch level ___ Windows 8.1 with April 2015 updates
[X] Windows 7 64 Patch level ___ Service Pack 1 with April 2015 updates
[X] Windows 7 32 Patch level ___ Service Pack 1 with April 2015 updates
[ ] Windows 2012 Server Patch Level ___
[ ] Windows 2008 Server Patch Level ___
[ ] Mac OS X x86 64 Version _____
[ ] Linux Distribution _____ Kernel _____
[ ] Other _____

5. Vulnerable Target application versions and reliability. If 32 bit only, is 64 bit vulnerable? List complete point release range.

Target Application / Version / Reliability (0-100%) / 32 or 64 bit?
Windows Media Center / 6.1.7601.17514, 6.3.9600.16384 / 100% reliable / both 32 and 64bits

6. Tested, functional against target application versions, list complete point release range.

Explain OS/ARCH/Target Version Reliability
Windows Vista, 7, 8.1 / 32 and 64bits / v.6.1.7601.17514 and 6.3.9600.16384 / Extremely reliable.

22. Description. Detail a list of deliverables including documentation.
Windows Media Center Specially crafted file arbitrary code execution vulnerability.
Windows Media Center contains a vulnerability that allows attackers to execute arbitrary code when a specially crafted Media Center file is opened. No further interaction required. This can be delivered by e-mail, web sites, instant messengers.

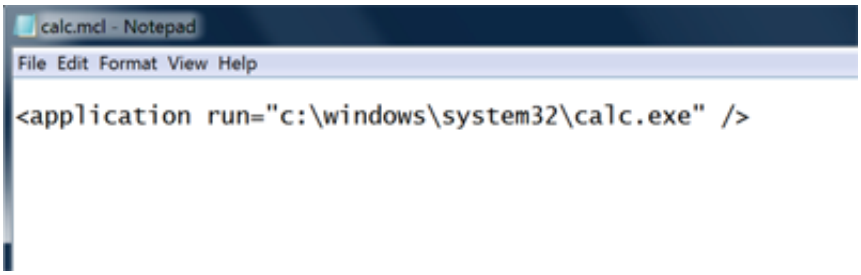
23. Testing Instructions
Download a specially crafted Windows Media Center file and open it. Arbitrary code is executed upon opening the file.

24. Comments and other notes; unusual artifacts or other pieces of information
Very reliable exploit.

The exploit relies on a specifically crafted Media Center link (.mcl) file that is used as attack vector. The file could be delivered in targeted attacks in various attack scenarios such as a spear phishing email, download from a website, via instant messaging applications.

Kenney Lu, Threats Analyst from Thrend Micro explained that it is quite easily to create the malicious file by using a common text editor like Notepad.

“It should be noted that the Windows Media Center file extension is .MCL. We found that it is easy to create .MCL files using *Notepad*. For example, we created a .MCL file that contained instructions that will launch the computer’s calculator. We have successfully reproduced and sent the related POC file to Microsoft, which they have addressed in this month’s Patch Tuesday.” explained Lu.



Due to the availability online of the Windows Media Center exploit since the Hacking Team hack, cybercriminals might start using it in targeted attacks, Trend Micro suggest users avoid opening any .MCL file.

"The leaked data has been made available for over a month now, following the Hacking Team leaks, and cybercriminals may use this exploit for future attacks. We recommend users avoid opening any files with the .MCL file extension, especially from unverified sources." states Trend Micro.

Pierluigi Paganini

(Security Affairs – Hacking Team exploits, Windows Media Center)

Breaking News Hacking Malware

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and "Digital Virtual Currency and Bitcoin".

PREVIOUS ARTICLE
Turla APT Group Abusing Satellite Internet Links