SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Microsoft Patches Windows Vulnerability Exploited in the Wild

By Eduard Kovacs on September 09, 2015

Microsoft has released a dozen security bulletins to patch more than 50 vulnerabilities affecting Windows, Internet Explorer, Edge, Office, Lync, Exchange Server, .NET Framework, Exchange Server, and Skype for Business Server.

The most important of the September 2015 bulletins is MS15-097, which addresses graphics component vulnerabilities that could allow remote code execution.

One of the flaws, a Win32k memory corruption issue that can be exploited for privilege escalation (CVE-2015-2546), has been exploited in the wild. The vulnerability affects all supported versions of Windows, including the latest Windows 10. Microsoft addressed this and three other Win32k memory corruption flaws by improving the way the Windows kernel-mode driver handles objects in memory.

According to Microsoft, there are four other vulnerabilities that have been disclosed publicly: a kernel ASLR bypass (CVE-2015-2529), a Windows Media Center RCE vulnerability (CVE-2015-2509), a .NET Framework integer overflow (CVE-2015-2504), and a memory corruption flaw in Edge and Internet Explorer (CVE-2015-2542).

The .NET integer overflow was disclosed in May by Dutch security firm Securify, but Microsoft hasn't rushed to release a patch because the bug is difficult to exploit.

The Media Center vulnerability came to light earlier this year following the breach suffered by Italian spyware maker Hacking Team. A leaked email referencing the exploit revealed that an attacker can execute arbitrary code by getting the targeted user to open a specially crafted Media Center link (.mcl) file.

Trend Micro reported this vulnerability to Microsoft on July 18 after finding the Media Center exploit in the Hacking Team leak.

"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," Trend Micro said in a blog post.

Other critical security bulletins released by Microsoft on Tuesday patch vulnerabilities in Internet Explorer, Edge, Windows Journal, and Office.

Craig Young, researcher at Tripwire, has pointed out that the Edge bulletin fixes a smaller number of flaws compared to the Internet Explorer bulletin.

"This is likely a consequence of how proficient researchers have become with fuzzing IE and may change as researchers revamp their toolkits to target Windows 10 and specifically Edge," Young told *SecurityWeek*.

The bulletins rated "important" address a denial-of-service (DoS) bug in Active Directory, privilege escalation flaws in the task manager, information disclosure and spoofing issues in Exchange Server, cross-site scripting (XSS) flaws in Lync Server and Skype for Business Server, and a Windows Hyper-V security feature bypass vulnerability.

Previous Columns by Eduard Kovacs:

Microsoft Patches Windows Vulnerability Exploited in the Wild
Researcher Discloses Zero-Day Flaws in Advantech WebAccess
Angler EK Uses Diffie-Hellman Protocol to Prevent Detection
Webroot, Avira Patch Flaws in Mobile Security Apps
Kaspersky Patches Critical Vulnerability in Antivirus Products

Tags:
NEWS & INDUSTRY Vulnerabilities

Subscribe to SecurityWeek

Most Recent Most Read

- Microsoft Patches Windows Vulnerability Exploited in the Wild
- Researcher Discloses Zero-Day Flaws in Advantech WebAccess
- NETGEAR Patches Vulnerability in Wireless Management System
- vCard Vulnerability Exposes WhatsApp Users
- Gozi Trojan Developer Pleads Guilty
- Rethinking Mobile Security - Why Apps Come First
- Angler EK Uses Diffie-Hellman Protocol to Prevent Detection
- Microsoft Acquires Cloud Security Startup Adallom
- Webroot, Avira Patch Flaws in Mobile Security Apps
- Kaspersky Patches Critical Vulnerability in Antivirus Products

Popular Topics

Information Security News
IT Security News
Risk Management
Cybercrime
Cloud Security

Application Security
Smart Device Security

Security Community

IT Security Newsletters
IT Security White Papers
Suits and Spooks
ICS Cyber Security Conference
CISO Forum
InfosecIsland.Com

Stay Intouch

Twitter
Facebook
LinkedIn Group
Cyber Weapon Discussion Group
RSS Feed
Submit Tip
Security Intelligence Group

About SecurityWeek

Team
Advertising
Events
Writing Opportunities
Feedback
Contact Us