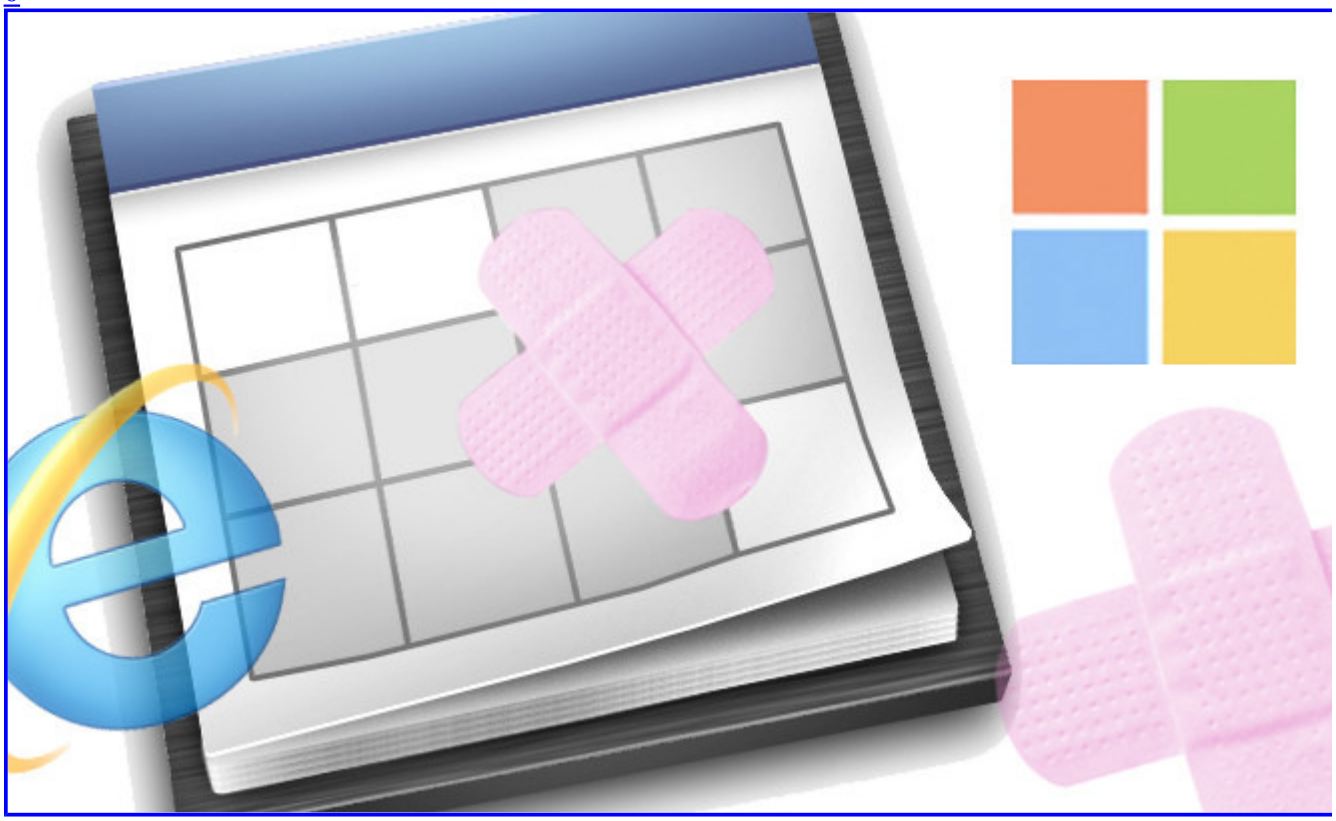
0



Microsoft August Patch Tuesday Addresses Critical IE, Exchange and Windows Flaws

Follow @mike_mimoso by Michael Mimoso August 13, 2013 , 2:28 pm

Microsoft took less than a month to incorporate an Oracle Outside In patch and fix a critically rated remote code execution bug in Exchange Servers. The Microsoft patch is among three critical bulletins—eight overall—released today as part of its August 2013 Patch Tuesday security updates.

Oracle patched Outside In with its July Critical Patch Update (CPU); the technology allows developers to turn unstructured file formats into normalized files. MS13-061 includes the Outside In Patch, which is part of the WebReady Document Viewing and Data Loss Prevention features on Exchange Servers. Exploits could allow an attacker to remotely execute code if a user previews or opens a malicious file using Outlook Web App (OWA). The attacker would have the same privileges as the transcoding services on the Exchange Server; that would be the LocalService account for WebReady Document Viewing and the Filtering Management service for the DLP feature. Both, however, run with minimal privileges.

Related Posts

Microsoft Pulls Back Critical Exchange Server 2013 Patch

August 14, 2013 , 4:51 pm

Microsoft Starts Countdown on Eliminating MD5

August 14, 2013 , 2:25 pm

Critical IE, Exchange Updates on Tap in August Patch Tuesday Release

August 8, 2013 , 3:28 pm

"If you run Exchange and your users have OWA, you should address this issue as quickly as possible," said Qualys CTO Wolfgang Kandek. Microsoft also recommends a workaround that turns off Outside In document processing.

MS13-059 is another cumulative patch for Internet Explorer and repairs 11 remotely executable vulnerabilities in the browser, including a sandbox bypass vulnerability discovered and exploited by VUPEN researchers during the Pwn2Own contest in March. IE 6-10 is vulnerable to exploit; Microsoft said it is not aware of any active exploits for any of these vulnerabilities.

The IE rollup includes patches for nine memory corruption vulnerabilities, as well as fixes for a privilege escalation flaw in the way in which the browser handles process integrity level assignment and an information disclosure cross-site scripting vulnerability in EUC-JP character encoding, Microsoft said.

"As usual with IE vulnerabilities, the attack vector would be a malicious webpage, either exploited by the attacker or it could be sent to the victim in a spear-phishing e-mail," Kandek said. "Patch this immediately as the highest priority on your desktop system and wherever your users browse the web."

The final critical bulletin, MS13-060, patches a Windows vulnerability in the Unicode Scripts Processor; the patch corrects the way Windows parses certain OpenType font characteristics. An exploit could allow an attacker to run code remotely if a user opens a malicious document or visits a website that supports OpenType fonts.

"A user would have to be induced to open a malicious file and this only affects Windows XP and 2003," said Ross Barrett, senior manager of security engineering at Rapid7. "Both of these issues should be patched ASAP." Microsoft also recommends two workarounds: either modifying the usp10.dll Access Control List to be more restrictive, or disabling support for parsing embedded fonts in IE.

The remaining bulletins were all rated Important by Microsoft.

- MS13-062 patches a privilege escalation vulnerability in Windows RPC, correcting the manner in which Windows handles asynchronous RPC messages. "Perhaps the most genuinely interesting vulnerability this month," Barrett said, adding that the bug is a post authentication issue in RPC. "Microsoft has described this as extremely difficult to exploit, which I can only assume is a challenge to exploit writers everywhere to prove them wrong."
- MS13-063 is another privilege escalation issue in the Windows kernel. Four vulnerabilities are patched in this bulletin, the most severe of which enables elevated privileges if an attacker is able to log in locally and run a malicious application. In addition to memory corruption bugs, one of the vulnerabilities in this bulletin enables an attacker to bypass Address Space Layout Randomization (ASLR), a memory protection native to the OS.

- MS13-064 patches a denial of service vulnerability in Windows NAT Driver. An attacker would have to send a malicious ICMP packet to a server running the NAT Driver services in order to exploit this bug, which affects only Windows Server 2012.
- MS13-065 also fixes a denial of service bug in ICMPv6; Vista, Windows Server 2008, Windows &, Windows 8, Windows RT and Windows Server 2012 are affected by this bug.
- MS13-066 patches an information-disclosure vulnerability in Active Directory Federation Services on Windows Server 2008 and Windows Server 2012. An exploit could force the service to leak information on the service and allow an attacker to use that information to try to log in remotely.

0
Categories: Microsoft

Leave A Comment

Your email address will not be published. Required fields are marked *

Name *

Email *

Comment

You may use these HTML tags and attributes: `<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <em> <i> <q cite=""> <strike> <strong>`

Post Comment

Notify me of follow-up comments by email.

Notify me of new posts by email.