West Texas Cyber Security Consortium

Microsoft Warns Of Zero-Day Vulnerability In Internet Explorer

Zero-day security vulnerability in IE 6-11 could allow remote code execution even if the user doesn't click on anything, Microsoft says.

Microsoft has discovered a zero-day vulnerability in most versions of Internet Explorer that already has enabled some attackers to execute code remotely on victim PCs, even without action by the end user. In a security advisory issued over the weekend, Microsoft reported that it "is aware of limited, targeted attacks that attempt to exploit a vulnerability" in IE 6, 7, 8, 9, 10, and 11. The vulnerability, which takes advantage of the way IE accesses an object in memory that has been deleted or has not been properly allocated, makes it possible for attackers to do remote code execution on a targeted machine, the advisory says.

"An attacker could host a specially crafted website that is designed to exploit this vulnerability through Internet Explorer and then convince a user to view the website," Microsoft says. "An attacker who successfully exploited this vulnerability could gain the same user rights as the current user."

Remote code execution means that attackers could distribute malware via a drive-by installation, "where simply looking at booby-trapped content such as a Web page or image file can trick IE into launching executable code sent from outside your network," notes Paul Ducklin, a researcher at security firm Sophos, in a blog posted Sunday. "There won't be any obvious warning signs, or 'Danger, Will Robinson' dialog boxes."

Using such an exploit, "a crook may be able to sneak malware onto your computer even if you don't take any obvious risks such as opening a suspicious attachment or agreeing to download a dubious-sounding file," he observes.

There is no patch yet for the vulnerability, but users can reduce the risk of exploit by turning off Active Scripting, disabling the Adobe Flash files that might be used as a lever for an attack, Ducklin says.

"The zero-day identified over this weekend requires an older vulnerability, identified in 2010, to be exploited in tandem in order for the attack to be effective," says Brandon Hoffman, vice president of cyber security at RedSeal, a security firm. "Organizations that have identified and prioritized this older vulnerability and patched it should be significantly more protected. Another key component is the ability of an attacker to move laterally across the network, imitating the user of the system compromised. Any organization that has properly segmented their network will be at low risk to sensitive data being accessed."

Lucas Zaichkowsky, enterprise defense architect AccessData, says the early exploit has been attributed to a group of attackers in China. "Because the exploit is only known to a Chinese group targeting specific organizations, Microsoft will likely wait until the next Patch Tuesday to make a patch available to the general public," he says.

Tim Wilson is Editor in Chief and co-founder of Dark Reading.com, UBM Tech's online community for information security professionals. He is responsible for managing the site, assigning and editing content, and writing breaking news stories. Wilson has been recognized as one ... *View Full Bio*

http://www.darkreading.com/vulnerabilities---threats/microsoft-warns-of-zero-day-vulnerability-in-internet-explorer/d/d-id/1234907