Microsoft issues advisory on Internet Explorer vulnerability

April 28 2014, by Nancy Owano

Microsoft is scrambling to repair a security hole in its Internet Explorer web browser, saying it has detected attempts to exploit the flaw

(Phys.org) —Microsoft issued a security advisory on Saturday regarding an issue that impacts the Internet Explorer Web browser. Microsoft said it was aware of limited, targeted attacks seeking to exploit the vulnerability of Internet Explorer versions 6 through 11.

The vulnerability is being characterized as a "remote code execution vulnerability." This allows remote code execution if users visit a malicious website with an affected browser. This is attack-by-lure, successfully convincing someone to go ahead and click a link in an email or instant message. An attacker can execute arbitrary code. Also, If the current user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Dustin Childs, a group manager within the Trustworthy Computing Group at Microsoft, weighed in on the matter Saturday, saying "We are monitoring the threat landscape very closely and will continue to take appropriate action to help protect customers."

He advised people to follow the "Protect Your Computer" guidance of enabling a firewall, applying all software updates and installing anti-virus and anti-spyware software. "Additionally, we encourage everyone to exercise caution when visiting websites and avoid clicking suspicious links, or opening email messages from unfamiliar senders."

As for future intentions, the company said, "On completion of this investigation, Microsoft will take the appropriate action to protect our customers, which may include providing a solution through our monthly security update release process, or an out-of-cycle security update, depending on customer needs."

This was also a busy weekend for Milpitas, California, based FireEye, the security company where its FireEye Research Labs had identified what it called a new Internet Explorer zero-day exploit used in targeted attacks. "The vulnerability affects IE6 through IE11, but the attack is targeting IE9 through IE11." The April 26 blog by Xiaobo Chen, Dan Caselden and Mike Scott said that "Threat actors are actively using this exploit in an ongoing campaign which we have named 'Operation

Clandestine Fox.' However, for many reasons, we will not provide campaign details. But we believe this is a significant zero day as the vulnerable versions represent about a quarter of the total browser market. We recommend applying a patch once available."

Collectively, last year, the vulnerable versions of IE accounted for 26.25% of the browser market, they wrote. "The vulnerability, however, does appear in IE6 through IE11 though the exploit targets IE9 and higher."

More information: www.fireeye.com/blog/uncategor … argeted-attacks.html

technet.microsoft.com/en-us/li … ecurity/2963983.aspx

© 2014 Phys.org

Citation: Microsoft issues advisory on Internet Explorer vulnerability (2014, April 28) retrieved 6 May 2024 from https://techxplore.com/news/2014-04-microsoft-issues-advisory-internet-explorer.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.