



Financial Cybercrime Task Force of Kentucky Department of Financial Institutions

Risk Advisory Bulletin

April 29, 2014

Bulletin Reference # B0414-02

Subject: Users of Internet Explorer versions 6 through 11 may be vulnerable to a Remote Code Execution Attack

The DFI's Financial Cybercrime Task Force of Kentucky (FCTFK) issues this Bulletin to the financial services industry in Kentucky related to a limited, targeted attack that attempts to exploit a vulnerability in Internet Explorer versions 6 through 11.

Background: On April 26, 2014, Microsoft announced discovery of a remote code execution vulnerability affecting Internet Explorer versions 6 through 11. The vulnerability exists in the way that Internet Explorer accesses an object in memory that has been deleted or has not been properly allocated. The vulnerability may corrupt memory in a way that could allow an attacker to execute arbitrary code in the context of the current user within Internet Explorer. An attacker could host a specially crafted website that is designed to exploit this vulnerability and then convince a user to view the website. Execution of this exploit has the potential of giving attackers the same user rights as the current user. If successful, an attacker who infects a PC running as administrator would have a wide variety of attacks open to them such as installing more malware on the system, creating new user accounts, and changing or deleting data stored on the target PC.

Recommendations: It is recommended that users of Internet Explorer 6 through 11 review Microsoft Security Advisory 2963983 for mitigation actions and workarounds. Microsoft reports that using Enhanced Mitigation Experience Toolkit (EMET) version 4.1 may help in mitigating the exploit. Additionally, the attack will not work without Adobe Flash. Disabling the Flash plugin within Internet Explorer will prevent the exploit from functioning. More details can be found at: [Microsoft Security Advisory 2963983](#).

Furthermore, the United States Computer Emergency Readiness Team (US-CERT), part of the U.S. Department of Homeland Security, issued a [notice](#) recommending that users and administrators enable Microsoft EMET where possible and consider employing an alternative web browser until an official update is available.

Additional information, including updates, can be found at [Microsoft's Security and Research Blog](#). If you have questions for the task force or would like to be placed on our alert list-serve, please contact dfi.reporting@ky.gov.

The Financial Cybercrime Task Force of Kentucky is a proactive, internal work group of DFI that focuses on best practice guidance and warnings for the financial services industry. The Task Force's goal is to identify and address emerging threats in cybercrime and security and to protect the integrity of the Kentucky financial system.

DFI, <http://kfi.ky.gov>, is an agency in the Public Protection Cabinet. For more than 100 years it has supervised the financial services industry by examining, chartering, licensing and registering various financial institutions, securities firms and professionals operating in Kentucky. DFI's mission is to serve Kentucky residents and protect their financial interests by maintaining a stable financial industry, continuing effective and efficient regulatory oversight, promoting consumer confidence, and encouraging economic opportunities.