Adobe Flash Player updates confront zero-day exploit

February 21 2014, by Nancy Owano

(Phys.org) —An Adobe Flash exploit has targeted three sites. Adobe Systems on Thursday announced knowledge of the exploit and what steps to take. The company assigned the CVE identifier CVE-2014-0502 to the vulnerability. Its security bulletin addressed updates for Adobe Flash Player in response to the zero-day exploit, responding to the incidents. Titled "Security updates available for Adobe Flash Player," the company said that "Adobe is aware of reports that an exploit for CVE-2014-0502 exists in the wild, and recommends users update their product installations to the latest versions," which were listed. The

attack, described as a zero-day Adobe Flash exploit, was discovered on February 13 by Milipitas, California- based security company FireEye.

Adobe's security updates included those for Adobe Flash Player 12.0.0.44 and earlier versions for Windows and Macintosh and Adobe Flash Player 11.2.202.336 and earlier versions for Linux. Adobe said that users of Adobe Flash Player 12.0.0.44 and earlier versions for Windows and Macintosh should update to Adobe Flash Player 12.0.0.70. Users of Adobe Flash Player 11.2.202.336 and earlier versions for Linux should update to Adobe Flash Player 11.2.202.341. Adobe Flash Player 12.0.0.44 installed with Google Chrome will automatically be updated to the latest Google Chrome version, which will include Adobe Flash Player 12.0.0.70 for Windows, Macintosh and Linux.

The announcement also provided guidelines for those using Adobe Flash Player 12.0.0.44 installed with Internet Explorer 10 and Internet Explorer 11. Users of Adobe AIR 4.0.0.1390 and earlier versions for Android were told to update to Adobe AIR 4.0.0.1628.

Adobe further explained how users can verify which version of Adobe Flash Player is installed on the user's system and instructions for updating software installations.

The FireEye team that spotted the exploit, meanwhile, offered some observation in a Thursday blogpost about the attack and the attackers. The attack targets were even evident in the headline, "Operation GreedyWonk: Multiple Economic and Foreign Policy Sites Compromised, Serving Up Flash Zero-Day Exploit." Commenting further, the team said, "As of this blog post, visitors to at least three nonprofit institutions—two of which focus on matters of national security and public policy—were redirected to an exploit server hosting the zero-day exploit. We're dubbing this attack 'Operation GreedyWonk.'" "They said they believe that GreedyWonk may be

related to a May 2012 campaign, "based on consistencies in tradecraft (particularly with the websites chosen for this strategic Web compromise), attack infrastructure, and malware configuration properties."-They said the group behind this campaign appeared to have sufficient resources, such as access to zero-day exploits, and "a determination to infect visitors to foreign and public policy websites."

Meanwhile, Microsoft wasted no time to issue a security advisory on Wednesday, regarding a vulnerability in Internet Explorer that could allow remote code execution. "Microsoft is aware of limited, targeted attacks that attempt to exploit a vulnerability in Internet Explorer 10. Only Internet Explorer 9 and Internet Explorer 10 are affected by this vulnerability."

More information: support.microsoft.com/kb/2934088
helpx.adobe.com/security/produ … layer/apsb14-07.html