Internet Explorer 11 vulnerability allows policy bypass

February 5 2015, by Nancy Owano

(Phys.org) —"Your authentication cookies could be up for grabs in the latest Internet Explorer 11 vulnerability," said Kareem Anderson in *WinBeta* on Wednesday. The targets are IE 11 on both Windows 7 and 8.1.

This vulnerability, noted Anderson, arrives in "an age of social networking and shortened URL links, driving traffic to malicious sites ladened with login stealing credentials." He added, "a vulnerability found in a fully patched version of Internet Explorer isn't helping matters." Microsoft is working on a fix. This is a Universal Cross Site Scripting (XSS) vulnerability where the Same Origin Policy (SOP) is bypassed.

Anderson said that the XSS bug allows attackers to steal login credentials while also injecting malicious content into the person's web-browsing session. A number of security sites pointed out this week that the attack in managing to bypass SOP amounted to bypassing a principle in Web applications models. Eduard Kovacs in *SecurityWeek* said that policy "prevents scripts loaded from one origin from interacting with a resource from another origin."

The Open Web Application Security Project discussed XSS in its overview: Cross-Site Scripting (XSS) attacks are a type of injection where malicious scripts are injected into otherwise trusted web sites. A malicious script is sent to an unsuspecting user, and the user's browser has no way of knowing the script should not be trusted and goes ahead to execute the script. The script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. The scripts can rewrite the content of the HTML page.

Threatpost further analyzed the bypass: "Using an iFrame, the bug appears to bypass same-origin policy, a key mechanism found in web application models that allows script running on pages from the same site to access each other's Document Object Model (DOM) but disallows access to other sites' DOM. Essentially it prevents code in a site's iFrame from being able to control content from that site. The vulnerability also bypasses standard HTTP-to-HTTPS restrictions, according to Joey Fowler, a senior security engineer at Tumblr."

Security Editor at *Ars Technica*, Dan Goodin, on Tuesday called the bug serious. A Microsoft representative issued an email to various tech sites saying, "We continue to encourage customers to avoid opening links from untrusted sources and visiting untrusted sites, and to log out when leaving sites to help protect their information."

Chris Brook in *Threatpost* went to the source of the discovery. "David

Leo, a researcher with the U.K.-based security consultancy firm Deusen publicized the bug on Full Disclosure over the weekend, linking to a demonstration which shows how it can be used to hack the content of a site, externally." In the proof-of-concept, after interaction from a user, closing a popup window and waiting seven seconds, the words "Hacked by Deusen" could be seen inserted into a site.