Vulnerability in Internet Explorer Could Allow Remote Code Execution

US-CERT (Computer Emergency Readiness Team) has issued an alert warning of a 0-day exploit for all versions of Internet Explorer that is currently being actively exploited. Microsoft says the vulnerability could be used to silently install malicious software without any help from users by merely browsing a malicious web site.

The University of Nebraska at Kearney ITS recommends using Firefox as your default browser, and especially recommends not using Internet Explorer until this vulnerability is patched.

IF you absolutely must run Internet Explorer, Microsoft recommends not logging into Windows as an administrator level user, running Internet Explorer in "Enhanced Protected Mode", and installing EMET (Enhanced Mitigation Experience Toolkit). EMET 3.0 does not mitigate this attack, so be sure you have the latest version (EMET 4.1) installed.

This is the first of many zero-day attacks and vulnerabilities that will never be fixed for Windows XP users. Microsoft last month shipped its final set of updates for XP. Unfortunately, many of the exploit mitigation techniques that EMET brings do not work in XP

For more information:

https://technet.microsoft.com/library/security/2963983

http://www.us-cert.gov/ncas/current-activity/2014/04/28/Microsoft-Internet-Explorer-Use-After-Free-Vulnerability-Being

http://krebsonsecurity.com/2014/04/microsoft-warns-of-attacks-on-ie-zero-day/