By Lucian Constantin, Softpedia.com

French vulnerability research company VUPEN Security reports the discovery of a use-after-free vulnerability affecting all versions of Internet Explorer that could possibly lead to code execution. According to the company's new "no more bugs for free" policy, details of the flaw will not be shared with Microsoft unless it pays.



"We Discovered the 10th Unpatched Use-after-free Vulnerability in MS Internet Explorer. IE 8/7/6 are all affected," a short announcement from VUPEN posted on Twitter reads. However, the research will only be available to its paying customers.

Use-after-free conditions occur when a program continues to use a pointer to a location in memory that has already been deleted or freed. According to an article from OWASP (Open Web Application Security Project) this type of vulnerability poses a very high risk level and has a high exploitation likelihood.

"The use of previously freed memory can have any number of adverse consequences - ranging from the corruption of valid data to the execution of arbitrary code, depending on the instantiation and timing of the flaw. If the newly allocated data chances to hold a class, in C++ for example, various function pointers may be scattered within the heap data. If one of these function pointers is overwritten with an address to valid shellcode, execution of arbitrary code can be achieved," is explained in the article.

VUPEN Security, which was previously known as FrSIRT, has been credited with discovering numerous critical vulnerabilities in widely deployed software, including Microsoft products. The company recently claimed to have discovered the first two vulnerabilities in the new Microsoft Office 2010 suite.

However, VUPEN is no longer willing to give away its research for free to the affected vendors. Instead, it practices responsible disclosure only with software developers that pay for the

information. "Why should security services providers give away for free information aimed at making paid-for software more secure?," Chaouki Bekrar, VUPEN's chief executive officer, commented for Heise Media.

The company continues to provide intelligence about the unpatched vulnerabilities, to various governments who are members of its Threat Protection Program, even if the vendor has not been informed. The information includes full binary analysis and detection guidelines.

This "no more bugs for free" policy appears to be a growing trend between security researchers. Proeminent white hat hackers like Charlie Miller, Alex Sotirov or Dino Dai Zovi have already already this stance since a year ago. Evgeny Legerov, founder of Moscow-based vulnerability research company Intevydis, who declared himself a responsible disclosure contester, compared the practice with doing free Quality Assurance work for vendors.