Vista contest offers cash for exploits

By Shaun Nichols on Jan 15, 2007 3:08PM

Security vendor offers US$8,000 for reports of Vista and IE7 flaws.

A US security firm is offering up to US$72,000 in bounties for the development of working exploits for Microsoft's Windows Vista and Internet Explorer 7.

IDefense has launched its latest Quarterly Vulnerability Challenge which offers researchers up to US$8,000 for reporting a working vulnerability allowing for remote code execution.

An additional US$2,000 to US$4,000 is available if the researcher can also deliver a working exploit.

IDefense has issued strict rules for the contest. No more than six vulnerabilities will be accepted, all of which must be present in the most recent versions of the software. Any exploit code must not contain any kind of malicious payload.

Flaws that allow for remote execution are among the most serious threats to users. Such outbreaks earn the highest alert levels from security monitoring sites, and are often referred to as 'critical' vulnerabilities.

Microsoft said that, although the company has a policy of not paying for vulnerability disclosures, it does not expressly support or oppose the iDefense programme.

"Microsoft does not oppose programmes that work through the established processes for responsible disclosure, and do not put customers at risk," a company spokesman told vnunet.com.

"Microsoft does not want to speculate on the motives of third-party researchers, but is committed to working with them closely on the issues that they bring to our attention."

Eric Sites, vice president of research and development at Sunbelt Software, told vnunet.com that he had mixed feelings about the contest.

While the iDefense programme rewards users for developing attacks, Sites warned that it also allows for the disclosure of vulnerabilities that may otherwise have been discovered by a malware author and launched without warning.

He pointed out that paying users for the rights to attack code gives one company a competitive advantage by allowing customers exclusive protection, but leaves users of other security programs vulnerable to attack.

What iDefense is doing is nothing new, according to Sites, who pointed to the thriving underground market for new exploits from developers of attack programs used by malware authors and distributors.

Vulnerabilities that allow for remote code execution are among the most sought after because they can give an attacker nearly limitless control over a system.

Dave Marcus, security research and communications manager at McAfee, explained the appeal of remote code vulnerabilities to vnunet.com in an interview last month after publishing a report on the recent increase in critical flaws.

"The critical vulnerability is definitely the holy grail," said Marcus. "It is the one that the malware writers and botnet operators want to use because it is the one that lets them inject the code."

Microsoft patched over 130 critical vulnerabilities in 2006, more than doubling the previous year's total.