

6 August 2008

By: Marius Oiaga, Technology News Editor



[Insight into the New Microsoft Vulnerability Exploitability Index](#)

A feature spawned as a consequence of user feedback

Microsoft's monthly release of security bulletins is bound to get a tad richer as far as the information provided to customers is concerned come October 2008. This will happen via the new Exploitability Index, introduced at the Black Hat USA 2008 conference on August 5, 2008. The new resource was spawned in accordance with end user feedback, which required additional data from the Redmond company related to the vulnerabilities patched every month across its products. In the end, the Exploitability Index is designed to provide guidance for the security patches that have to be a priority in terms of deployment.

"Microsoft will evaluate the potential exploitability of vulnerabilities associated with a Microsoft security update. Microsoft will apply a value to the vulnerabilities associated with a Microsoft security update. Information will then be published in the Exploitability Index as part of the monthly Microsoft security bulletin summary," the company informed. There are no less than three Exploitability Index Values, namely: "Consistent Exploit Code Likely," "Inconsistent Exploit Code Likely," and "Functioning Exploit Code Unlikely." Microsoft is already informing customers on cases where it detects attacks in the wild, or the existence of exploit code, or proof-of-concept code. In this regard, the Exploitability Index will attempt to approximate what are the chances for exploit code to follow on the heels of the security patches. "Consistent Exploit Code Likely - this means analysis has shown that exploit code could be created in such a way that an attacker could consistently exploit that vulnerability. This would make the vulnerability an attractive target for attackers; therefore, it is more likely that exploit code would be created. As such, customers who have reviewed the security bulletin and have determined its applicability within their environment might treat a vulnerability with this value as a higher priority," Microsoft revealed. In the same manner, "Inconsistent Exploit Code Likely" will be used to indicate that even with exploit code available a potential attacker would not be able to take full advantage of the security holes in the targeted software. What this value implies is that any attack making use of exploit code would be sufficiently unreliable for it not to be worth while. "Functioning Exploit Code Unlikely - this means analysis has shown that exploit code which functions successfully is unlikely to be released. While an attacker could create exploit code that could trigger the vulnerability and cause abnormal behavior, it is unlikely that an attacker would be able to create an exploit that could successfully exercise the full impact of the vulnerability. Therefore, once customers have reviewed the security bulletin to determine its applicability within their environment, they might prioritize this update below other vulnerabilities within a release," Microsoft added.