

7 April 2008

By: Marius Oiaga, Technology News Editor

[Windows XP SP3 Gets Its First Taste of Vulnerabilities](#)

According to Symantec



Windows
Microsoft

The [third and final service pack for Windows XP](#) is not even out the door, and security company Symantec has already warned of a security vulnerability impacting XP SP3. With the advent of Windows Vista, Microsoft has started beating the drum of the increased security of its latest Windows client in comparison to XP SP2. Throughout 2007, the Redmond company has offered ample proof of the fact that Vista RTM was affected by less than half the volume of vulnerabilities in contrast to XP RTM. This trend seems to continue with Vista Service Pack 1 and XP SP3. The proof of concept of a new bug impacting Windows Explorer is now available in the wild, with potential exploits affecting XP SP3. "The bug affects the code that parses Word documents in order to extract and display summary information (for example, document type, author, title, etc.). A malformed property record in the DocumentSummaryInformation stream of the Word document will cause Explorer to access an invalid pointer when parsing the file, causing the process to crash because of a memory access violation. In our tests we found that Microsoft Word XP, currently updated with SP3 and the latest patches, seems to be vulnerable to this bug, which causes Word to crash due to a 'divide by zero' exception," revealed [Andrea Lelli](#), Symantec Security Response Engineer. According to Symantec, the bug is not Critical as it only allows for denial-of-service (DoS) attacks. Users browsing in Windows Explorer or attempting to open a malformed Word document will trigger the DoS exception, causing both applications to crash. Lelli stated that it is highly unlikely that an attacker will be able to execute malicious code on an affected system via exploiting the bug. "We took a look at the problem in the crafted proof-of-concept .doc and we think that the problem lies in the DocumentSummaryInformation container of a Word document stream. This object contains information about the document, such as the title and the author, and Windows Explorer will display this information when needed. For example, when we select a document from Explorer with the status bar visible, this information will be displayed on the status bar. This means that Explorer parses the document, reads the DocumentSummaryInformation, and parses the information stored inside," Lelli said. "Windows XP Service Pack 3 Release Candidate 2 Refresh can be downloaded from [here](#).