MS First Look: Word 2007 Not Bitten by Bugs

April 12 2007

Microsoft says it is still investigating reports of posted security holes, but it has found no evidence that the Office 2007 suite is vulnerable to the reported flaws.

Microsoft says a preliminary investigation into reports of vulnerabilities in its Office 2007 suite has produced no evidence of a threat to users.

Reports of new security holes in MS Office have been made public on known exploit sites, including information about four bugs posted on one site. Microsoft has not released specific information about the vulnerabilities, citing potential risk to users.

"Microsoft's initial investigation has found that none of these claims demonstrate any vulnerability in Word 2007 or any Office 2007 products," a company spokesperson said April 11. "Our investigation into the possible impact of these claims on other versions of Microsoft Office is continuing."

The reported flaws were uncovered by Mati Aharoni of Offensive-Security.com, in Israel. He said he was not searching for vulnerabilities in Word, but stumbled upon them while developing Offensive-Security.com course materials.

"I ran a character substitution script on several Windows file formats and was left dazed by the results," he said. "The vulnerabilities I released to the public were the least dangerous of my findings - most resulted in DOS only - actually getting code to execute via these bugs is highly improbable."

Two of these documents show how Word 2007 could trigger a "CPU exhaustion." A third vulnerability, also concerning Word 2007, could supposedly allow remote code execution. The fourth alleged vulnerability, which concerns the ".hlp" extension for Windows help files, could cause a heap overflow condition.

Aharoni said he has received several messages from others confirming that the bugs crashed Word 2007. He posted screenshots of the crashes or CPU exhaustion conditions on his blog, and expressed confusion as to why Microsoft seems unable to reproduce the conditions.

Through the company spokesperson, Microsoft stated the company may issue a security advisory or update if it is deemed necessary.

Karthik Raman, a researcher at McAfee, in Santa Clara, Calif., wrote in a blog post April 10 that the timing of publicizing of the potential

vulnerabilities on exploit sites may not be coincidental. "This is yet another time that zero-day flaws have been published around a Patch Tuesday, possibly to maximize the public's exposure to these flaws until the next month's Patch Tuesday," Raman wrote.

Andrew Storms, director of security operations at nCircle, in San Francisco, said the issue of responsible disclosure is a never-ending debate within the security space. He advocates responsible disclosure, defined as reporting a vulnerability to a vendor first and allowing the company a chance to fix it.

"It comes down to the question, Does responsible disclosure to the vendor deliver a better product? Does it force the vendor to fix it more quickly?" he said.

Aharoni said he has little patience for the formal disclosure process after having had disappointing experiences with it in the past.

"Microsoft has made huge leaps in security in the past years and I appreciate that," he said. However, he said, "As a Microsoft customer, I would like to see bugs patched quicker."