

18 January 2006

By: Alex Muradin, Editor, Software Reviews



## [Full Disclosure Speeds Up Microsoft Patches](#)

*This isn't Watergate and Deep Throat, but disclosing information has gotten quite the reputation.*

Public Disclosure of Microsoft flaws make the Redmond giant fix the problem quicker. No one likes to have their dirty laundry publicly displayed and Microsoft Corp. is no exception. A recent look back at Microsoft's [patching practices](#) has been scrutinized by Brian Krebs, a staff writer at the Washington Post. He's taken a look back at how quickly and effectively Microsoft reacted when a "critical" security update had been identified. According to his numbers, in 2005 it took Microsoft 50% more time to issue [critical software patches](#) compared to 2003. In 2003 it took roughly three months for Microsoft to get a patch out the door when problems were reported to the privately. In 2004, the number it took for them to issue skyrocketed to 134.5 days, which also remained very similar in 2005. Microsoft's tune quickly changes when outsiders take charge of the situation and start publicly posting security flaws. It seems like over the past few years their reaction time has sharpened when news of a flaw spreads through outside sources or isn't given to Microsoft privately. The numbers gathered seemed to show a trend as well. In 2003, their reaction time to an outside security flaw posting was on average 71 days, in 2004 it only took 55 days and finally in 2005 it was down to 46 days. Although it may appear that full disclosure is quite an effective means of making them release a patch sooner, Microsoft prefers the information to remain private until they have issued a patch to fix the issue. In 2003, they learned of 8 critical Windows vulnerabilities, in 2005 that number was down to 4. A reason why they prefer this method would be because they typically tend to rush the fixes rather than review them properly. An example would be the "Blaster" worm fiasco where they produced a [patch](#) for that vulnerability in just 38 days. Two days after Microsoft released the patch, researchers found the flaw in three other areas of the operating system that the initial fix did not address. Stephen Toulouse, a security program manager at Microsoft, said "It was a conscious decision at the time to release that patch so quickly, but we later looked back and decided we really should have conducted a more thorough review process." So the question people are asking now is how does one get a patch out quickly in order to protect the customers while also getting it right the first time? Microsoft is the only company that can answer that.