

5 January 2009

By: Marius Oiaga, Technology News Editor

Security  
Microsoft

## [MD5 Hashing Algorithm Hole Not a Microsoft Product Vulnerability](#)

### *The company says*

At the end of the past year, limited details on a security hole in MD5 were made public in a demonstration of collision attacks aimed at digital certificates signed using the hashing algorithm. The security researchers who demoed the attacks did not release the actual particulars on the [MD5 hashing algorithm vulnerability](#) to the public. However, Microsoft felt the need to deliver additional information to its customers, while emphasizing that the issue affected the entire industry and not just its software products.

"This is not a vulnerability in our products, it is in fact an issue that affects the industry as a whole. Over Christmas, Microsoft has also been working with several certificate authorities to make them aware of the issue and encourage them to move to more robust technologies. We hope this advisory helps address some of your concerns," [Maarten Van Horenbeeck](#), Microsoft Security Response Center program manager, revealed.

The vulnerability in the MD5 hashing algorithm allowed for attacks against X.509 digital certificates, Microsoft informed. In this manner, browsers that interpret CA certificates supplied by Certification Authorities in order to ensure a high level of security over HTTPS (Hypertext Transfer Protocol Secure) via the SSL (Secure Sockets Layer) cryptographic protocol can be fooled into informing users that the website they are visiting can be trusted completely, even though it is in fact malicious in nature.

"Attacks on MD5 have been known for some time, but were never considered to be very practical. This type of attack allows the generation of additional digital certificates with different content, but the same digital signature as an original certificate," Van Horenbeeck added.

Since the security researchers failed to make available the cryptographic background of the demo-attack, Microsoft estimated that the disclosure did not boost the risk for customers. However, the Redmond company advised all interested parties to stop signing their certificates using the MD5 algorithm, and to migrate to more secure alternatives, such as SHA-1, SHA-256, SHA-384 or SHA-512.