

Security Flaw Shows Microsoft Passport Identities Can't Be Trusted

John Pescatore, Avivah Litan

A serious security flaw shows that Microsoft Passport identities could be easily compromised. Financial institutions and other enterprises should replace or augment Passport until at least November 2003.

NEWS ANALYSIS

Event

On 8 May 2003, Microsoft acknowledged a major security flaw in its Passport Internet user-authentication service. An independent researcher in Pakistan first identified the flaw. It could theoretically have enabled unauthorized access to any of the more than 200 million Passport accounts used to authenticate e-mail, and e-commerce and other transactions. Microsoft indicates it has resolved the problem and does not know of any accounts that were breached.

Analysis

This huge security flaw couldn't have emerged at a worse time for Microsoft Passport, which has struggled to gain enterprise and consumer acceptance ever since it went live in 1999. Microsoft failed to thoroughly test Passport's security architecture, and this flaw — uncovered more than six months after Microsoft added the vulnerable feature to the system — raises serious doubts about the reliability of every Passport identity issued to date.

Whether any attackers exploited this flaw before Microsoft patched the problem is important to enterprises that depend on Passport identities, but it doesn't affect the actions they must take to limit the damage. As with any piece of software with serious security flaws, more vulnerabilities will likely surface in Passport. For this reason, Gartner recommends that financial institutions, credit card issuers, retailers and other enterprises that use Passport for any meaningful business purpose immediately:

- Break all Passport connections until at least November 2003 or until Microsoft can prove that its security is adequate. Or invest in an additional, more secure form of authentication for all issued Passport identities.
- Contact all customers who use Passport and make them aware of Microsoft's recommendations for Passport account holders (see www.microsoft.com/security/passport_issue.asp).

Enterprises considering Passport services should delay adoption until at least November 2003 or until Microsoft has completed a thorough security review of Passport, including outside reviewers.

This discovery deals a major blow to Microsoft and the Liberty Alliance, which have not yet succeeded in getting the consumer e-commerce market to accept identity services of this type. Gartner surveys have shown that consumers and enterprises have already seen more risk than value in Passport and Liberty. The serious vulnerability in Passport will likely further delay any meaningful demand for such services until at least 4Q04. Microsoft can reduce this impact and regain market confidence by submitting Passport's code to a full open-source review.

Analytical Sources: John Pescatore and Avivah Litan, Gartner Research

Written by Terry Allan Hicks, Gartner News

Recommended Reading and Related Research

- "Privacy and Security Still Challenge Microsoft Passport" — Consumer distrust prevents widespread acceptance of Passport. **By John Pescatore, David Smith and Avivah Litan**
- "Microsoft Passport: Many Registrations, but Few Users" — Gartner research shows that real-world use of Passport will remain very limited through 2003. **By Avivah Litan**

(You may need to sign in or be a Gartner client to access all of this content.)

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Level 7, 40 Miller Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Latin America Headquarters
Av. das Nações Unidas 12.551
9 andar—WTC
04578-903 São Paulo SP
BRAZIL
+55 11 3443 1509