

Multiple Vulnerabilities found in Microsoft .Net Passport Services

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-05/0022.html>

From: Qazi Ahmed (qa_at_PAKCERT.ORG)

Date: 05/08/03

Date: Thu, 8 May 2003 07:19:44 +0500

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

PakCERT Security Advisory PC-080503

<http://www.pakcert.org/advisory/PC-080503.txt>

Multiple Vulnerabilities found in Microsoft .Net Passport Services

May 08, 2003

BACKGROUND

“Microsoft® .NET Passport is a Web-based service designed to make signing in to Web sites fast and easy. .NET Passport enables participating sites to authenticate a user with a single set of sign-in credentials, eliminating the need for users to remember numerous passwords and sign-in names.”

“Since its launch in 1999, Microsoft® .NET Passport has become one of the largest online authentication systems in the world, with more than 200 million accounts performing more than 3.5 billion authentications each month. .NET Passport participating sites include NASDAQ, McAfee, Expedia.com, eBay, Cannon, Groove, Starbucks, MSN® Hotmail, MSN Messenger, and many more.”

Benefits of Using .Net Passport Services

- “Use one name and password to sign in to all .NET Passport-participating sites and services.”
- “Store personal information in your .NET Passport profile and, if you choose, automatically share that information when you sign in so that participating sites can provide you with personalized services.”

DESCRIPTION

PakCERT has discovered two serious vulnerabilities in Microsoft .Net Passport Services, which if exploited, affects over 200 million users worldwide. Using these vulnerabilities and the single sign-in feature of Microsoft .Net Passport, an attacker can completely take control of a

NT–Bugtraq: Multiple Vulnerabilities found in Microsoft .Net Passport Services

user's account including Hotmail email account, personal information, credit card numbers, shopping lists etc and use it on any of the .Net Passport participating web sites.

Issue One: Bypass Security Questions

An attacker can bypass the security questions asked before resetting the password. When Microsoft Hotmail/.Net Passport users forget their passwords, they have to fill out a web form that requires their email address, state, zip code and country. After submitting the correct information users are prompted to answer the secret question they entered during their signup for the service.

As a result of this vulnerability, Microsoft Hotmail/.Net Passport users who rely on questions like “What’s my name?” or “What’s my favorite color?” could find themselves loosing their accounts.

Issue Two: Password Reset Vulnerability

An attacker can reset any Microsoft Hotmail/.Net Passport user account with no prior information like state, zip, country, answer to the secret question and the old password. Normally, a user has to answer the security questions and than answer the secret question if he wants to reset his password. By exploiting this vulnerability, an attacker can submit a specially crafted URL to get the password reset instructions and reset any user's password.

TECHNICAL DETAILS

Due to the nature of this vulnerability and the fact that there is no fix available yet, no technical details are being made available with this advisory. Full technical details will be made available on our website once the vulnerability is fixed by Microsoft. Please note that we were forced to release this information public as these vulnerabilities are actively being exploited in the wild and are one of the most severe vulnerabilities ever found in Microsoft Hotmail/.Net Passport.

FOUND BY: Qazi Ahmed & Shoaib Rehman

AUTHOR: Qazi Ahmed

DISCLAIMER

The information within this paper may change without notice. Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties with regard to this information. In no event shall the author be liable for any damages whatsoever arising out of or in connection with the use or spread of this information. Any use of this information is at the user's own risk.

NT-Bugtraq: Multiple Vulnerabilities found in Microsoft .Net Passport Services

PakCERT Contact Information:

Email: pakcert@pakcert.org
Phone: +92-21-5872445 - 47
Fax: +92-21- 5378505
Postal Address:
PakCERT
Office #5, 3rd Floor, Plot No. 6-C
7th Zamzama Commercial Lane
Phase-V, D.H.A
Karachi, Pakistan

REFERENCES

- <http://www.passport.com/>
- <http://www.hotmail.com/>
- <http://www.msn.com/>
- <http://www.microsoft.com/net/services/passport/>
- <http://www.microsoft.com/net/services/passport/business.asp>

oo
Delivery co-sponsored by IP3 Inc.
oo
SECURITY QUESTIONS? We've got answers...Apply for a scholarship and become
TICSA certified.

Do not miss your opportunity to discover solutions to what our participants have identified as their top 5 IT Security Challenges. You will return to work better prepared to put into place an effective security strategy utilizing the latest security tools, bookmarks and URL's.

<<http://www.ip3seminars.com>>

oo