

Securiteam: [NEWS] Vulnerability Enables Passport Account Hijackings (No Secret Question)

# [NEWS] Vulnerability Enables Passport Account Hijackings (No Secret Question)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0001.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 07/01/03

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 1 Jul 2003 14:57:01 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at [canadasales@beyondsecurity.com](mailto:canadasales@beyondsecurity.com)

-----  
Vulnerability Enables Passport Account Hijackings (No Secret Question)  
-----

## SUMMARY

A newly disclosed vulnerability could enable attackers to reset the password and hijack older Microsoft Corporation .Net Passport accounts. A "Secret Question" feature that is used to validate the identity of a user who needs to reset his account password can be manipulated by attackers on Net Passport accounts that were set up before Microsoft implemented the Secret Question feature, according to a message posted by Victor Manuel Alvarez Castro, who identified himself as a security consultant.

## DETAILS

Microsoft did not immediately respond to requests for comment.

Accounts created since the Secret Question feature was implemented require the account owner to establish a secret question to retrieve their password, so not all .Net Passport users are affected by the flaw.

## Securiteam: [NEWS] Vulnerability Enables Passport Account Hijackings (No Secret Question)

It has been "a couple of years" since the Secret Password feature was implemented, Castro said.

The vulnerability requires that attackers know both the e-mail address and home country of the account owner. In the case of U.S. based accounts, an attacker would also need the state and zip code of the account owner.

Those conditions make it more difficult to exploit the vulnerability, according to Rafael Núñez, a senior research scientist at Scientech de Venezuela in Caracas, Venezuela, who is known online as "[RaFa]".

However, given the estimated 200 million .Net Passport accounts and the length of time that services like Hotmail have been online, there may be a large number of accounts affected by the Secret Question vulnerability, Núñez said.

The attack would be especially useful for targeted attacks by those familiar with the victim, he said.

Once in control of the victim's .Net Passport account, an attacker could pose as that person online, using the victim's e-mail account or other services such as Microsoft's MSN instant messenger to pose as the victim online and perform "social engineering" attacks to collect other sensitive information, Núñez said.

This is the second vulnerability affecting .Net Passport in as many months. In May Muhammad Faisal Rauf Danka, a security researcher in Pakistan, reported a flaw in a function that enabled Passport users who had forgotten their password to change it using an e-mail message sent to an address associated with their Passport account.

The flaw enabled an attacker to have the password update e-mail sent to an e-mail address of their choice, and required little more than knowledge of their victim's e-mail address to use.

In that instance, repeated e-mail messages from Danka to Hotmail support went unanswered, prompting him to disclose the problem publicly.

Similar confusion about the correct procedure for reporting vulnerabilities may be at play in the latest revelation as well, which was not first disclosed to the Redmond, Washington, company, according to Núñez, who learned of the vulnerability from a Spanish language vulnerability discussion list on Friday.

Núñez worked with Castro to direct him to the proper security group in Redmond, but the researcher released the information on the Internet instead, he said.

### ADDITIONAL INFORMATION

Securiteam: [NEWS] Vulnerability Enables Passport Account Hijackings (No Secret Question)

The information has been provided by deepquest and  
<mailto:adf@code511.com> adf.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

**DISCLAIMER:**

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.