

Full-Disclosure: Re: [Full-Disclosure] Hotmail & Passport (.NET Accounts) Vulnerability

Re: [Full-Disclosure] Hotmail & Passport (.NET Accounts) Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-04/0811.html>

From: Jon (jbistogood_at_hotmail.com)

Date: 04/20/04

To: <full-disclosure@lists.netsys.com>

Date: Tue, 20 Apr 2004 20:51:47 +0100

<https://register.passport.net/emailpwdreset.srf?lc=1033&em=vanecarolina13@hotmail.com&id=&cb=&prefem=careverga7@.com&rst=1>

And youâ?Tll get an email on attacker@attacker.com'

Sure you didnt mean to replace one of the email addresses in there with 'attacker@attacker.com'?

Even if you do, it doesn't seem to work. I tried switching each one for my own and no such luck. I only recieved an email when both the addresses were set to my hotmail account.

That means it's only any good if you have access to the users hotmail account but don't know their password in the first place.

Jon

----- Original Message -----

From: "fernando escobar" <careverga7@hotmail.com>

To: <full-disclosure@lists.netsys.com>

Sent: Tuesday, April 20, 2004 2:27 PM

Subject: [Full-Disclosure] Hotmail & Passport (.NET Accounts) Vulnerability

> *I am forwarding this as it may impact people whom depend on MSN or
> passport systems for business reasons. Contrary to what at
> least one of the full-disclosure follow-ups reports, it does work.*

>

> *D*

>

>

> ----- Forwarded message -----

> *Date:* Wed, 7 May 2003 19:50:51 -0700 (PDT)

> *From:* Muhammad Faisal Rauf Danka

> *To:* full-disclosure@lists.netsys.com

> *Subject:* [Full-Disclosure] Hotmail & Passport (.NET Accounts)

Vulnerability

>

Re: [Full-Disclosure] Hotmail & Passport (.NET Accounts) Vulnerability

Full-Disclosure: Re: [Full-Disclosure] Hotmail & Passport (.NET Accounts) Vulnerability

> *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=vanecarolina13@hotmail.com&id=&cb=&prefem=careve>

>

> *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*

>

>

> *Charla con tus amigos en línea mediante MSN Messenger:*

Re: [Full-Disclosure] Hotmail & Passport (.NET Accounts) Vulnerability

Full-Disclosure: Re: [Full-Disclosure] Hotmail & Passport (.NET Accounts) Vulnerability

> <http://messenger.latam.msn.com/>

>

>

> *Full-Disclosure – We believe in it.*

> Charter: <http://lists.netsys.com/full-disclosure-charter.html>

>

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>