

## Re: Active Directory password external use

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2005-09/0005.html>

---

**From:** Mike Mitchell ([mmitchel\\_at\\_myra.com](mailto:mmitchel_at_myra.com))

**Date:** 09/01/05

Date: Wed, 31 Aug 2005 16:39:30 -0700

To: [focus-ms@securityfocus.com](mailto:focus-ms@securityfocus.com)

I was involved in a single-signon password strengthening project where we sync'ed domain passwords with those required by a back end app database. We hooked MS' notification package facility as per <http://support.microsoft.com/default.aspx?scid=kb:en-us:Q161990> (and others, I'm sure).

My c routine (as a dll) gets a clear text copy of the password from the DC when ever a password change is initiated. According to the MS docs, I return TRUE or FALSE indicating whether or not I liked new password. For ease of maintenance, I also pass the password off to an external processor (a script, whose task it is to update the back end database password 'seemlessly').

Some more info here: <http://is-it-true.org/nt/registry/rtips165.shtml>, or e-me.

Mike

Manuel Fernandes wrote:

- > *What agent or daemon will capture this – is it part of an identity*
- > *management (IdM) system?*
- >
- > *Yes, some IdM agents can capture the password in clearat the DC and*
- > *distribute it before it is encrypted.*
- >
- > *Without getting specific to a product or technology, most mature*
- > *systems have provisions to interact with msgina.dll*
- >
- > -----Original Message-----
- > *From: Matthew Farrenkopf <farrenkm@ohsu.edu>*
- > *To: focus-ms@securityfocus.com*
- > *Sent: Wed, 31 Aug 2005 08:21:47 -0700*
- > *Subject: Re: Active Directory password external use*
- >
- > *"Rodrigo Blanco" <rodrigo.blanco.r@gmail.com>:*
- >

SecurityFocus Microsoft: Re: Active Directory password external use

>> *I am currently doing a project that requires using the Active  
>> Directory users' password for other purposes other than just  
>> workstation logon or share access.*  
>>  
>> *What I would need to do is detect password change / reset events on  
>> the domain, capture the new password and send it to another  
>> application. This could be done with an agent or daemon running on the  
>> DC machine.*  
>>  
>> *The question is, when a users' password is changed / resetted, is it  
>> possible to externally capture this event and make use of the password  
>> before it is stored in a non-reversible format inside the active dir.?*  
>>  
>> *What security implications would this have, and what security measures  
>> would you propose for such an agent?*  
>  
>  
> *Seems like a lot of work for a small reward. We have several Web  
> applications  
> that authenticate directly against the domain controller. I've never  
> done it  
> before, but there's probably someone that has (and I am actively  
> trying to learn  
> how to do it).*  
>  
> *Why not do that?*  
>  
> *Matt*  
>  
>  
>  
>  
-----  
>  
>  
-----  
>  
>  
>  
-----  
>  
>  
-----  
>  
>  
-----  
-----