

Re: Adding XP in another partition users into Vi\$ta

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.windows.vista.security/2008-10/msg00382.html>

- *From:* "FromTheRafters" <erratic@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Sun, 19 Oct 2008 17:54:40 -0400
-

Thanks again Jimmy.

I guess you can't always believe what you read.

"Jimmy Brush" <jb@xxxxxxx> wrote in message
<news:%23zD98JZMJHA.4600@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

The statement about there being no API to do it is just plain wrong. I guess sometimes the left hand doesn't know what the right hand is doing :).

If Windows didn't support some mechanism for allowing a group of users to set the owner on a file, the Windows backup program could not correctly restore backups.

One can always remove this capability by not granting Administrators the restore privilege.

– JB

"FromTheRafters" <erratic@xxxxxxxxxxxxxxxxxxxx> wrote in message
<news:e2cOBjXMJHA.3744@xxxxxxxxxxxxxxxxxxxxxxxxxxxx>

It was this bit that got me thinking that...

"The Owner tab shown in Figure 12.19 has no option for giving ownership to another individual. If that were possible, an unscrupulous user could take ownership, do something wrong, and then cover his tracks by giving ownership to someone else. To prevent that from happening, the operating system does not support a give ownership operation at any level not in the user interface, not in application programming interfaces. It is true that a program can write new information in the Owner field of an object's security descriptor if the process has WRITE_OWNER access to the object, but WRITE_OWNER access permits the caller to change ownership only to the user SID in the caller's access token or, if the user is a member of the Administrators group, to the Administrators SID. Thus it is never

Re: Adding XP in another partition users into Vi\$ta

possible to give ownership of an object to another user. If you want to transfer ownership of an object, you must give another user permission to take ownership and then wait until the other user takes it."

"Jimmy Brush" <jb@xxxxxxx> wrote in message
news:%237ugJRKMJHA.4772@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Yup :). You have to hold the restore privilege (admins have it by default).

This isn't new functionality to Vista, it was just never exposed in the UI before.

<http://support.microsoft.com/kb/245153/EN-US/>

I am not aware of any auditing enhancements.

– JB

"FromTheRafters" <erratic@xxxxxxxxxxxxxxxxxxxx> wrote in message
news:%23RqSSMJMJA.3744@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Can you confirm this? It was my understanding that you can only grant the permission for another to take ownership and not simply assign ownership to another (for auditing purposes to avoid someone taking ownership, making nefarious changes and then assigning ownership to a scapegoat).

...again, this was from the W2K link – but I don't see why that would change in Vista (unless they've improved on the audit trail).

"Jimmy Brush" <jb@xxxxxxx> wrote in message
news:Os9bZ1%23LJHA.3080@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Also, you can assign ownership to an arbitrary user or group in Vista through the ACL editor UI, with the appropriate rights

Re: Adding XP in another partition users into Vi\$ta

of course.

– JB

"FromTheRafters"

<erratic@xxxxxxxxxxxxxxxxxxxx>

wrote in message

news:exUKOk%23LJHA.4772@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Thanks for
your answer
Jimmy.

Having read
this:

<http://www.microsoft.com/technet/prodtechnol/windows2000serv/res/>

...it had me
wondering
how things
may have
changed re
Vista.

"Jimmy
Brush"

<jb@xxxxxxx>

wrote in
message

news:eSHYjY%23LJHA.4772@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hello,

That's
an
excellent
question.

The
scenarios
are
different
depending
on
whether
you
are
logged
in

Re: Adding XP in another partition users into Vi\$ta

as
a
standard
user
or
an
administrator.

When
logged
in
as
a
standard
user,
when
you
elevate
you
are
logging
in
with
the
credentials
you
supply
to
the
elevation
prompt
and
the
elevated
program
is
running
under
those
credentials.
So,
there
are
actually
2
SIDs
involved
and
things
work
as

Re: Adding XP in another partition users into Vi\$ta

you
described.

Things
get
tricky
when
you
are
logged
in
as
an
administrator.

In
this
case,
you
only
have
one
SID,
but
you
get
2
tokens
with
different
privileges
when
you
log
in.
The
tricky
part
is
that
in
the
restricted
token,
your
group
membership
in
the
administrators
group
is

Re: Adding XP in another partition users into Vi\$ta

set
to
only
be
considered
for
deny
permissions.

So,
the
following
scenario
could
happen:

–
You
are
logged
in
as
an
admin

–
You
are
running
a
program
that
is
not
elevated
that
wants
to
change
the
permissions
on
a
file

–
You
are
not
granted
access
to
the

Re: Adding XP in another partition users into Vi\$ta

file
in
any
permission
–

The
administrators
group
owns
the
file

You
would
not
be
able
to
use
the
non–elevated
program
to
change
the
permissions
on
the
file,
because
your
membership
in
the
administrators
group
is
being
ignored
when
the
system
is
deciding
if
you
should
be
able
to
have

Re: Adding XP in another partition users into Vi\$ta

read/change
acl
access
to
the
file
by
virtue
of
being
the
owner.

Of
course,
this
scenario
probably
wouldn't
happen
in
real
life...
the
program
should
know
to
throw
a
UAC
prompt
to
get
elevated.

In
addition,
there
is
also
the
concept
of
integrity
levels.
Most
non-elevated
processes
are
assigned

Re: Adding XP in another partition users into Vi\$ta

medium
integrity,
while
an
elevated
process
is
assigned
high
integrity.
Every
file
is
assigned
an
integrity
level.

A
process
can
only
write
to
a
file
that
has
an
equal
or
lower
integrity
level
than
the
process,
regardless
of
what
permissions
are
set
or
who
the
owner
is.

So,
an

Re: Adding XP in another partition users into Vi\$ta

un-elevated
process
(medium
integrity)
could
not
write
to
or
change
the
permissions
on
a
file
that
has
high
integrity,
even
if
your
SID
had
full
control
of
the
file
and
was
the
owner.

(There
are
no
files
by
default
that
have
high
integrity).

–
JB

"FromTheRafters"

Re: Adding XP in another partition users into Vi\$ta

<erratic@xxxxxxxxxxxxxxxxxxxx>
wrote
in
message
news:u3YSsJ9LJHA.276@xxxxxxxxxxxxxxxxxxxxxxxx

"Man-wai
Chang
ToDie
(33.6k)"
<toylet.toylet@xxxxxxxx>
wrote
in
message
news:%235UxUA0LJHA.5660@xxxxxxxxxxxxxxxxxxxxxxxx

Under
Vi\$ta:
First,
I
removed
all
accounts
that
could
access
folder
X.
Then
I
let
user
Y
to
take
control
of
the
folder,
including
subfolders.
I
only
want
Vi\$ta's
user
Y
to
access
that

Re: Adding XP in another partition users into Vi\$ta

folder.

Was
user
Y
elevated
when
you
took
ownership?

I've
been
wanting
to
ask
the
experts
in
this
group
about
this
for
awhile
anyway,
so
here
it
goes.

When
an
SID
is
created
by
a
limited
user
with
an
admin
token
(elevated
standard
account)
is
the
"owner"

Re: Adding XP in another partition users into Vi\$ta

field
different
than
it
would
be
without
the
admin
token?
In
other
words,
is
it
only
possible
to
be
accepted
as
the
"owner"
if
you
are
attempting
access
as
that
same
user
again
also
elevated?

Then
I
boot
back
into
XP:
XP's
Administrator
as
well
as
user
could
no

Re: Adding XP in another partition users into Vi\$ta

longer
access
folder
X,
unless
I
let
XP's
Admin
to
take
control
of
folder
X.
But
if
I
did
that,
when
I
booted
back
into
Vi\$ta,
Vi\$ta's
user
Y
could
no
longer
access
folder
X.

Have
you
tried
elevating
Vista's
Y
user
when
attempting
access
of
folder
X?
Not

Re: Adding XP in another partition users into Vi\$ta

because
it
needs
elevated
privileges,
but
because
it
needs
"owner"
to
match
the
SID
–
just
in
case
the
split
token
is
what
is
causing
this
confusion.
Thereafter
you
should
be
able
to
allow
any
standard
user
account
you
want
to
assume
ownership.

Sorry
if
this
isn't
helpful,
but
maybe

Re: Adding XP in another partition users into Vi\$ta

you
would
have
better
luck
in
the
micro\$oft.pubic.windoze.vi\$ta.insecurity
newsgroup.