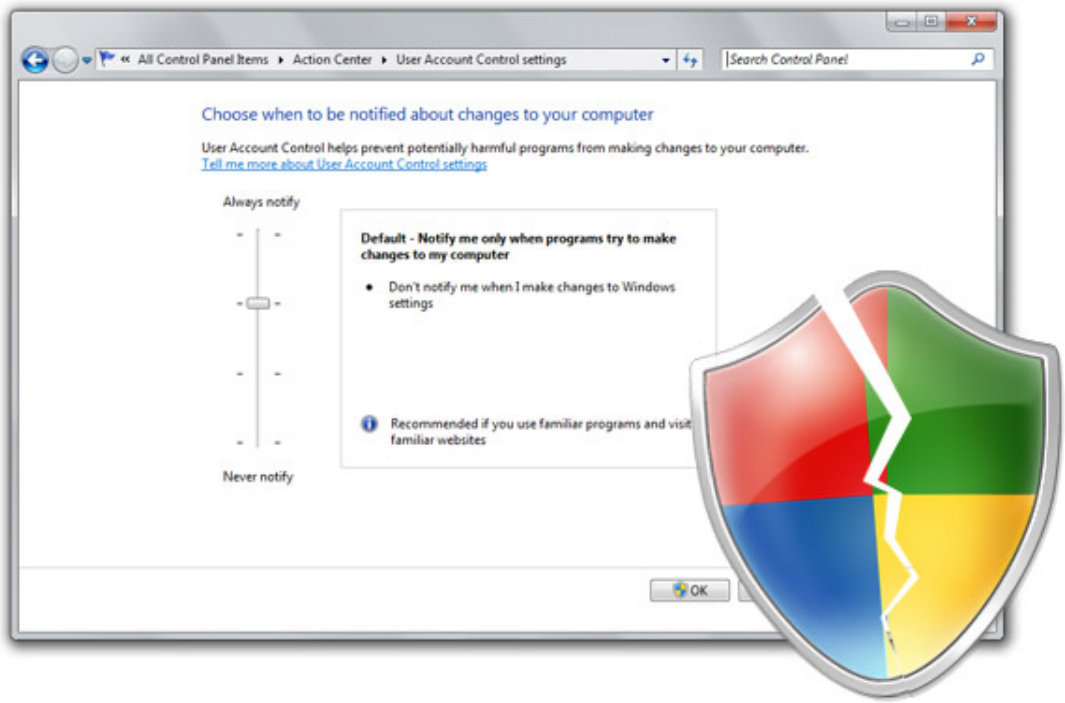
January 30, 2009

Sacrificing security for usability: UAC security flaw in Windows 7 beta (with proof of concept code)



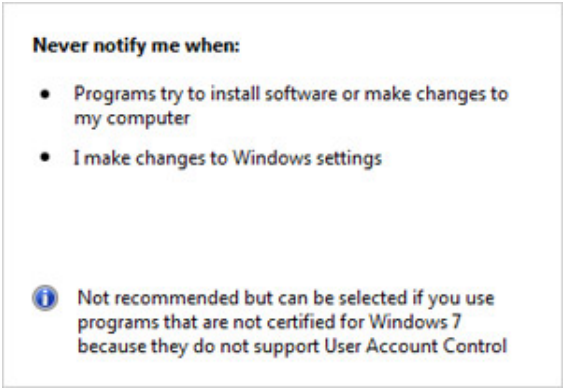
This is dedicated to every ignorant "tech journalist" who cried wolf about UAC in Windows Vista. A change to User Account Control (UAC) in Windows 7 (beta) to make it "less annoying" inadvertently clears the path for a simple but ingenius override that renders UAC disabled without user interaction. For the security conscious, a workaround is also provided at the end. First and foremost, I want to clear up two things.

First, I was originally going to blackmail Microsoft for a large ransom for the details of this flaw, but in these uncertain economic times, their ransom fund has probably been cut back so I'm just going to share this for free.

Secondly, the reason I'm blogging about this flaw is not because of its security implications – it is blatantly simple to fix – but Microsoft's apparent ignorance towards the matter on their official Windows 7 beta feedback channel by noting the issue as "by design" and hinting it won't be fixed in the retail version. A security-minded 'whistleblower' came forth to ask me if I could publicize this issue to maybe persuade them to change their mind. And that's what I'm doing.

Now for a bit of background information on the changes to UAC in Windows 7. By default, Windows 7's UAC setting is set to "Notify me only when programs try to make changes to my computer" and "Don't notify me when I make changes to Windows settings". How it

distinguishes between a (third party) program and Windows settings is with a security certificate. The applications/applets which manage Windows settings are signed with a special Microsoft Windows 7 certificate. As such, control panel items are signed with this certificate so they don't prompt UAC if you change any system settings.

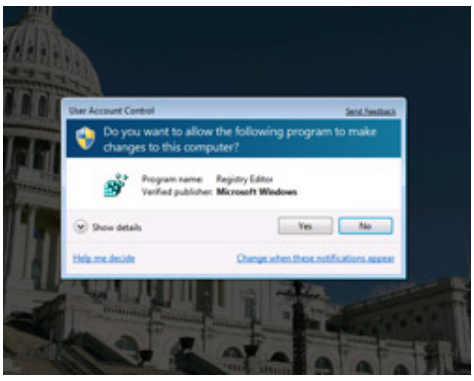


The Achilles' heel of this system is that changing UAC is also considered a "change to Windows settings", coupled with the new default UAC security level, would not prompt you if changed. Even to disable UAC entirely.

Of course it's not a security vulnerability if you have to coerce the user into disabling UAC themselves (although sweet candy is exceptionally persuasive), I had to think "bad thoughts" to come up with a way to disable UAC without the user's interaction. The solution was trivial, you could complete the whole process with just keyboard shortcuts so why not make an application that emulates a sequence of keyboard inputs.

With the help of my developer side-kick Rafael Rivera, we came up with a fully functional proof-of-concept in VBScript (would be just as easy in C++ EXE) to do that – emulate a few keyboard inputs – without prompting UAC. You can download and try it out for yourself here, but bear in mind it actually does disable UAC.

We soon realized the implications are even worse than originally thought. You could automate a restart after UAC has been changed, add a program to the user's startup folder and because UAC is now off, run with full administrative privileges ready to wreak havoc.



This is the part where one would usually demand a large sum of money but since I'm feeling generous, there is a simple fix to this problem Microsoft can implement without sacrificing any of the benefits the new UAC model provides, and that is to force a UAC prompt in Secure Desktop mode whenever UAC is changed, regardless of its current state. This is not a fool-proof solution (users can still inadvertently click "yes") but a simple one I would encourage Microsoft to implement seeing how they're on a tight deadline to ship this.

Having UAC on at the policy as it is currently implemented in Windows 7 is as good as not having it on at all.

Until when Microsoft decides to fix this, if they do at all, beta users of Windows 7 can also apply a simple fix. Changing the UAC policy to "Always Notify" will force Windows 7 to notify you even if UAC settings change. Annoying, but safe.

Update: I must credit Aubrey from WindowsConnected.com for also touching on this issue briefly today.

Update 2: Microsoft has officially responded to my concerns and continues to insist the functionality is "by design", dismisses the security concerns and again leans towards they will not be addressing the issue for the final release of Windows 7.

Update 3: A reader has kindly asked me to highlight a particular condition for this to work, the user must be in the "Administrative" user group, and not in the "Standard" user group where they will be prompted for a administrative password. In defense of the seriousness of the issue, the Vista and Windows 7 default user group is "Administrative" and I'm sure that's what most home users are running.

Update 4: Microsoft's Jon DeVaan has posted a response on the official Windows 7 blog with an extensive look at the UAC system in Windows 7 and their decision on the default security policy. In conclusion, they continue to stand by their decision and does not indicate they will change the default UAC policy.

Update 5: Microsoft fixed this.

← Older Newer →

219 insightful thoughts

Eric Rodewald

January 30, 2009 at 4:41 pm

Scary. I can't imagine that they would ignore this flaw unless there is more to the story we aren't hearing. This sort of compromise in a released product would be discovered on a Monday and fixed on Patch Tuesday.

January 30, 2009 at 4:44 pm

JT

On their lowest 3 settings, the UAC prompts aren't a security boundary at all. If explorer.exe can silently elevate to write a shortcut into the allusers startup directory, you can call the same COM object and do the same work from your own app. *shrug*.

January 30, 2009 at 4:59 pm

Albert

I've always been a lone advocate for UAC. Mainly because it protects "average" users…and there are a lot more of them than us. However, it will be very difficult for Microsoft to address this issue. It needs to somehow please all of those people at the top (who find UAC annoying and have the power to publicize their opinions to the point it determines the realities of "average" people) and keep end-users safe, so Windows itself can be more secure. Like Long said, "Annoying, but safe."

January 30, 2009 at 5:11 pm

Taimur Asad

i now hear a wo-wo coming from Microsoft.

January 30, 2009 at 5:34 pm

Thor Marius K.H

Wouldn't a potential fix be to disallowing any application to interact with the signed programs? Forcing human interaction?

January 30, 2009 at 5:36 pm

@Thor Marius K.H: That would fix it, but then has the potential to break application compatibility if they relied on this capability. Also, they

★Long Zheng

already have a solution called “Secure Desktop”, where it dims your screen, but its off because UAC never prompts you.

January 30, 2009 at 5:38 pm

That UAC icon sure is scary. I like Vistas UAC icon more than Windows 7.

Afizz

January 30, 2009 at 5:40 pm

@Afizz: I hope you realize the “break” was intentionally edited by myself, and is not the default icon in Windows 7 🙂

★Long Zheng

January 30, 2009 at 5:50 pm

Isn’t releasing this informaiton and code irresponsible?

Mark

January 30, 2009 at 5:59 pm

@Mark
I’m guessing that if someone has the skill to write a virus in a high level language, they would be able to do something as simple as VB, as well figure out the flaw.

Cullen D

January 30, 2009 at 6:13 pm

@Mark: People have already tried to get Microsoft to fix this via non-public means, but that hasn’t worked for them which is why they’ve come looking for support. The way I see it, it would be irresponsible of me to know about this and not get it changed before its final.

★Long Zheng

January 30, 2009 at 6:29 pm

Fowl

I thought this when I first heard about the UAC changes in 7, but I'd always assumed that Microsoft knew what they were doing… I trusted them, they were very specific about how UAC in Vista was done the way it was to avoid this sort of thing – so it seemed logical to me that they had found some workaround and it was still secure. Apparently not.

Humph. ;(

January 30, 2009 at 6:34 pm

Albert

@Afizz: I don't know…they're sporting my school's colors 😀

January 30, 2009 at 7:27 pm

Sven

Long, thanks for publishing this.

I'm one of the people who has bugged this issue on the Connect website. My bug received nearly fifty validations, and at over forty votes had an average rating of 4.9 out of 5. The bug was the highest rated bug on the Windows 7 Connect website.

Then Microsoft, much to my astonishment, closed it as "by design". Hopefully drawing some more attention to this issue will achieve some results.

January 30, 2009 at 8:37 pm

Michael Teper

http://blogs.msdn.com/oldnewthing/archive/2009/01/21/9353310.aspx

January 30, 2009 at 8:42 pm

Don

If memory serves Vista used to be more like that before it became final, but then accessibility software vendors complained that it would stop their products from working. The solution used was that the accessibility software would then run in a higher integrity level which was even able to control dialog boxes such as the UAC prompts.

The rule for allowing a program to affect another program is that it can do so if it has the same integrity level or higher. So I can see why this has been labeled “by design”.

January 30, 2009 at 8:48 pm

Christian

Interesting find Long. Thanks for posting this.

January 30, 2009 at 10:00 pm

Fowl

@Michael Teper: The whole point is that a program that doesn’t have admin rights, can get them without user interaction/consent.

January 30, 2009 at 10:30 pm

Don

OK, so after looking into this it’s not done how I thought it would be done. The problem I see is that the window where you can change the UAC setting is owned by “explorer.exe” which runs with medium integrity. This is why the VB script is able to inject keyboard events into that window.

Oops.

January 30, 2009 at 11:06 pm

Yikes. Hopefully this gets fixed before RTM.

Jason Cox

January 30, 2009 at 11:26 pm

Unless this is changed before RTM, it looks like I'll be changing UAC mode to "always prompt" on all my Windows 7 installations in the future!

Matt Sharpe

January 30, 2009 at 11:48 pm

good job on bringing this to everyones attention, and its sad that MS is stating this was done by design, lets hope by pulling this into the light, sumthin will be done about it.

lets just hope this gets fixed by RTM!

peas
cityboy

dj_cityboy

January 31, 2009 at 12:13 am

People have complained that UAC is useless, but the second someone gets the other half of their complaints, being "less annoying" (and let me tell you, run XP the way it is meant to be run – in a limited account, and you will know that UAC is a gift – the complainers are only admitting being mentally retarded when it comes to security) then it actually becomes useless!

sigh Looks like I'll have to do some baseline configuration when I first install a Windows 7 box because the default sucks.

Yert

January 31, 2009 at 12:19 am

Perhaps it's only "by design" in the beta to ease testing?

Fowl

January 31, 2009 at 12:32 am

Albert G.

Thanks for posting this. I really hope MS fixes this before going retail, but if not, at least we'll know now what setting to use.

Oh, and the Vista's UAC haters never really had any idea what they were talking about anyway.

Thanks again.

January 31, 2009 at 1:00 am

Good_Bytes

Let's all send a feed back explaining this issue!
With the high number, Microsoft is sure to look into it.

January 31, 2009 at 1:02 am

★Long Zheng

@Good_Bytes: That is the problem, everyone DID send feedback about this issue, and it had a lot of votes, but Microsoft shut it down and marked it as "by design". Which is why we're now here.

January 31, 2009 at 1:18 am

Good_Bytes

Ah, now I undertsand..
But I think we need try again.. I mean look under Vista when you maximize a window/program teh boarders turns blackish and the taskbar turns black opaque as well. Few people complained, Microsoft said it was by design, but they did change in Windows 7, making the programs on Windows 7 unusable….

I am sure more pressure will make Microsoft change it.

January 31, 2009 at 2:40 am

Gus

Anybody who complains about UAC itself is just too plain stupid.
On all my machines, Windows and Linux, I run as unprivileged user, and it's not much of a problem. OK, you need to tweak permissions on one or two registry entries and one or two files, but it sure is a lot less work than setting up your OS after a malware attack.
The real problem is how UAC was _implemented_ in Vista: if you want to, suppose, copy a folder with 2 EXEs into c:\programs, you have to answer several prompts, because UAC in Vista is not clever enough to see this as one action:
1 – You are about to do something that needs administrative privileges – OK to proceed?
2 – You are about to create a folder in c:\programs – OK to proceed?
2 – You are about to copy a program to c:\programs – OK to proceed?
This is the REAL UAC WTF – Windows should be clever enough to see this as ONE action:
1 You are about to create a folder in C:\programs and copy two program files into it – OK to proceed?

January 31, 2009 at 2:49 am

Gus

I forgot something else to add to my above post:

Software that needs full privileges for doing non-administrative tasks is just badly written. Ever since people changed from Windows 98 to 2000, separation of user accounts and separate access have existed for most users – that's almost 10 years ago!!!
IMHO, Microsoft should have discouraged users from running as admin years ago and should never have created the "power users" group.
If software on other OSs can live without these privileges, Windows-SW should be able to do that as well. Maybe it's time to get rid of all the old and badly written stuff, or talk to your suppliers about it.

January 31, 2009 at 2:57 am

W7

You'd think they have to fix this in the next release now that this has come to light. Submitting feedback on the issue can't do any harm, even

if it got us here in the first place.

January 31, 2009 at 3:23 am

This problem can be solved even simpler than your suggestion.

Jeroen

Just like Cardspace, put the dialog to change the UAC settings on the secure desktop, so programs cannot interact with the UAC settings dialog. The problem is that changing the checks of whether or not to skip a UAC prompt will probably introduce more problems and a whole lot of work…

January 31, 2009 at 3:41 am

Bug it simple.

Imran

January 31, 2009 at 3:59 am

Long Zheng,

Larry Seltzer

So could they block this attack by making the UI behind the applet that actually imposes the change force the user to confirm in secure desktop?

January 31, 2009 at 5:17 am

Gizmodo has also mentioned/linked to this post and credited you.

Jordan

January 31, 2009 at 5:23 am

Wow, forgot how much crap I left behind when I went to OSX.

Todd Jolley

MS will never be able to secure their OS until they bite the bullet and make a clean break from how they architect their OS and move to a paradigm that the Unix and Unix-type OS's have used for over 20 years.

UAC is nowhere near as annoying on OSX: You try to install a program that accesses system level resources, you get a single prompt to put in your system password. The first time a program is run, you get a pop-up indicating the source of the program and where it came from. After allowing it to run, you never get bugged again.

We're coming up on 8 years of OSX (March 24th) with a grand total of 1 Trojan that was just released on pirated iWorks '09 last week, and 1 other malware program from a couple of years ago that only infects a Mac after the user did 5 specific steps, in order, to actually install it and give it access to the system.

Linux and Unix are pretty much in the same boat. Maybe there is something to this whole "users are not system admins by default" thing? Maybe MS should fix the underlying design flaw and deal with some broken software packages while the vendors fix thier packages. Suffer the pain and fix the issue once and for all.

January 31, 2009 at 5:30 am

Good_Bytes

Great another macfanboy troll coming to a windows topic to show of how Mac is better, when it clearly is not, and is full of issues. End of conversation.

January 31, 2009 at 6:13 am

frymaster

"Maybe there is something to this whole "users are not system admins by default" thing?"

what a brilliant idea. Why don't we make all people run as limited users by default but, like the linux "sudo" command, allow them to escalate to admin priviledges without having to log off and log in again! we could call it "uac"…..

January 31, 2009 at 6:17 am

Marc Klink

I suppose this is a big deal to some, but to me it also focusses attention on what has been wrong with Windows for (now, with 7 almost out) the past 2 iterations. Microsoft makes things difficult , or impossible, to do, and forces the users to yield or not use the product. The company does this to ostensibly save the user from 'all the bad things' out to get them in cyberspace. In doing so, those who are not idiots, and have an idea of how to keep a machine from being compromised are left with systems that are effectively taken over by the Microsoft hive mind method of doing things.

With each change lately, a few more will not surrender to the idea of Microsoft telling them where their programs can reside on their hard drives, how they can't have a hierarchical structure of programs in the way that they please, or how those programs can be accessed in a start menu.

Many will accede to the stupid and capricious will of the designers at Microsoft, who publicly criticize Unix structures, and then quietly and clumsily copy them for their own wants. These sheep will do so because they are sheep, but not everyone will.

Rather than have all of this 'lockdown' affecting everyone, perhaps it would be better to suggest to Microsoft to, instead of having multiple flavors of 7 with few differences, to simply have a different distinction. Windows 7 for Beginners, the OS that will allow MS to dictate EVERY major and minor element, under the guise of safety, and Windows 7 Advanced, for those who wish to actually use the hardware and software they buy without annoyances, in the way they see fit.

January 31, 2009 at 7:28 am

BA

So basically, get the user to run a program to disable UAC to then run a program that can do stuff to the system.

What if I don't run your program? Can you disable my UAC without any effort on my part?

January 31, 2009 at 7:58 am

Stuart Kelly

It is a same that such a serious security issue has not yet been addressed. Hopefully Microsoft will fix this before the release candidate.

January 31, 2009 at 9:01 am

Dennis

Microsoft should not allow the average user to disable the UAC control and they should design it so that users have to enter their passwords, thereby making it more similar to the *nix OS designs. If users had no choice but to enter their password each time they made some change that could affect their system files, it might condition them into being more careful about the changes on the system that they allow. A prompt out of nowhere when you haven't performed any recent actions would make more users suspicious and hopefully prevent a few infections or worse.

January 31, 2009 at 10:14 am

Daniel

A more responsible way to log these kinds of things, rather than taking it into your own hands…. http://www.zerodayinitiative.com/

Great find, just imo, not done the right way.

January 31, 2009 at 10:32 am

Mark

@longzheng – thanks, i didnt realise it had been reported to Msft earlier through private feedback

January 31, 2009 at 10:42 am

James G.

Prompting for a password will just condition users to enter their password. Why don't you stick to science, instead of unix-fanboyisms. It is better that a user not enter his/her password all the time, for obvious reasons.
I blame the UAC haters for this issue in Win7, they complained and spammed message boards over and over until MS gave in, and now it's insecure, and now the haters complain about THAT. Figures. MS should fix this, but probably won't. There's too many clueless lusers out there who don't want the trouble of pressing yes/no and getting a screen blink for them to change it now. I really don't blame MS, how can MS make a secure OS when everyone complains and names it 'the top 25 tech flop' etc. for their trouble, MS has to give the market what it wants, and the stupid lusers want an insecure OS. Just thank god we can switch it to secure mode in a few mouse clicks.

January 31, 2009 at 11:57 am

ac

windows 7 will come with free malware protection which I think will compensate for uac changes

January 31, 2009 at 12:20 pm

Corrine

Enter my hero, Bill Pytlovany, developer of WinPatrol!

WinPatrol to Plug UAC Security Flaw In Windows 7

January 31, 2009 at 12:53 pm

canchin

This is just another reason why nobody should bother with any new OS release until at least Patch 2.0.

I moved from W98 to XP after Patch 2.0 came out and I haven't had a single problem. I wont bother with Vista – just like I never bothered with "Bob" or "Me" – and will not give MS my money until Windows 7-Patch 2.0 because I refuse to give MS my money so that I can pay them to allow me to be a Beta Tester.

I figure, sometime in perhaps 4th quarter 2010 W7 will be ready for prime time.

If there are no early adopters due to reports like this one showing MS isn't interested in fixing the bugs found by Beta Testers and tech-savvy researchers, and MS sees themselves looking at another Vista debacle of low adoption percentages, perhaps they'll actually listen to those like Mr. Zheng who are trying to help them.

January 31, 2009 at 1:32 pm

duane baker

i have one comp. with xp and my new comp. with vista. my vista is the only one on the internet. all i do is read email & surf the web. on line. i play war games, single player. i do not think i will update to windows 7 because vista is bad enough. in fact think i will just drop the internet altogether because i:m already seeing another rip off by microsoft. they are laying off 30 thousend people. why dosn:t bill gates give those people a few billions he made off of people. instead of laying them off. what happens when people don:t jump on the band wagon of windows 7? i think dumbes like me who bought vista should get a free upgrade to windows 7? thanks for listening to my gripe.

January 31, 2009 at 1:42 pm

duane baker

THANKYOU”””””’

January 31, 2009 at 1:55 pm

Jeffrey Byron

haha first things I noticed was, that is not the icon for the security shield in Windows 7 on the first image, its the new yellow blue yellow blue shield not the Vista red green blue yellow shield.

Anyway I'm sure Microsoft will work on this, that's why they have beta's. I'm not worried at all.

January 31, 2009 at 2:44 pm

Steve Coleman

And to think just how long it took MS to “fix” the shatter attack (sending messages to a priv window to get admin privs, broken since NT 4.0 and finally fixed in Vista) and then they turn right around and reimplement a similar “feature” like this within two years time.

January 31, 2009 at 3:00 pm

Satish

I feel like few others here that MS decided to label this bug “By Design” because of certain accessibility products or the functions used in certain products of large corporate users/ISV’s, which require automatic elevation at certain stages of their functioning without user interference.

Hopefully MS could patch this in a cleaner manner by
1. Prompting UAC to users when UAC settings are changed.
2. Providing a Group policy by which other programs / admins who want to use automatic elevation can achive it . (May be even program names and signatures which will be allowed to do it is in Group Policy.)
3. Prompting UAC to users when group policies regarding UAC are changed. (which will be only one time … say … during program installation.

January 31, 2009 at 3:29 pm

Aubrey

I’m glad others besides me realize how important this is. Thanks for the link and for helping to get the issue out in the open. Hopefully Microsoft will recognize what a huge problem this is before RTM.

January 31, 2009 at 3:49 pm

martin

so whats the code name of windows 7?
i found this http://tinypic.com/view.php?pic=2uj7cxv&s=5

January 31, 2009 at 7:49 pm

loop

what the hell are they thinking…critical vulnerability so lets ignore it… something fishy going on here..that or “by design” means that they have no way of fixing it or you either have to be protected fully or no protection at all through uac….no middle road here..idiots!!!!

January 31, 2009 at 9:45 pm

someone anonymous

Well, the Action Center runs as a service, so what if you set the Action Center to Automatic and deny everyone else permission to change the startup state of the service in the registry?

January 31, 2009 at 10:49 pm

SireeBob

sigh I think it was just a case of TL;DR (too long; didn’t read) for the Microsoft employee looking at the bug report. I suggest submitting another, but if this problem keeps getting attention, somebody at Microsoft with half a brain should hear about it anyway. These people are conditioned to assume all users are stupid, and sometimes they don’t even give bug reports like this a second thought.

January 31, 2009 at 11:29 pm

Master Guru

Long,

Thanks for the update, but would all you blogging folks now please correctly show home users how to create a user account and what to do when prompted for admin credentials….it is the right thing to do.

February 1, 2009 at 1:40 am

Good_Bytes

@martin , this is fake.
Longhorn is Vista. (NT 6.0 (yea still NT even if in reality it's a new core… it should NNT (New NT, or New New Technology), or some other name… but wtv)
Windows 7 is NT 6.1. Project name of Windows 7 is…. Windows 7. Why 7? because the the 7th release of Windows for non-servers computers.

February 1, 2009 at 1:53 am

Good_Bytes

@SireeBob , that is an unfair statement.
Do you think the programmers get these tings? No they don't!
It pass trough filters (people deleting useless feedback like "YOU SUKX!!!!!111111 one one one one", then it gets regrouped, and goes to some manager (like most companies they don't know jack shit about computers), read them and decides teh follwoing:
– "I have to see the project engineer working on the appropriate part of Windows to seek for a solution"
– "It looks too complicated to fix, screw it"
– "I know best! I think the project engineer would agree that it was by design.. I won't bother them"
– "It's an easy fix, let's fix it"
– "We got better priorities, because I think that UAC (which I have no clue what that is) is unimportant"

February 1, 2009 at 2:42 am

agcd07

Doesn't the user still have to download and copy the application into their startup group or registry to get it to emulate the keyboard shortcuts in the first place? Wouldn't automating that process trigger the UAC alert? Maybe this is why Microsoft doesn't really care about fixing it., because it can never be fully automated.

February 1, 2009 at 3:40 am

Yes, if you put the security bar to the max, I think (Won't that be Vista behavior?)

Good_Bytes

February 1, 2009 at 4:09 am

If the programs must have this “certificate” how did you manage to get the certifcate for the program you and Rafael created?

Albert

February 1, 2009 at 4:24 am

This is what happens when your developers are from other countries, taking orders from U.S. management, and do not understand the requirements.

Bill Melater

February 1, 2009 at 8:34 am

A more responsible way to log these kinds of things, rather than taking it into your own hands…. http://www.zerodayinitiative.com/

Daniel

Great find, just imo, not done the right way.

You got your awnser that its by design, your not happy with it… dont use it. Simple really.

February 1, 2009 at 9:32 am

It’s on Digg, should go digg it: http://digg.com/security/UAC_Security_Flaw_in_Windows_7_Microsoft_Will_NOT_

Craig Matthews

February 1, 2009 at 9:34 am

@agcd07: No. They can download a malicious application (VBS, EXE) and save it to their desktop. Then double click on it. No UAC prompts at

★Long Zheng

all.

February 1, 2009 at 9:43 am

agcd07

@Long Zheng: If the user has to download and double click on it, then what's the security risk? How is this a security flaw? Next they're going to say your surge surpressor has a security flaw because the end user could switch it off while the computer is on.

February 1, 2009 at 9:48 am

Good_Bytes

@agcd07 , no because Vista doesn't have this issue…
It's sad to see Vista more secure than Win7.

February 1, 2009 at 9:54 am

★Long Zheng

@agcd07: You're assuming hackers and people with truly evil intent are as considerate and forthcoming as Rafael and I.

The point is, the code that is used to disable UAC entirely can be run in low-privilege mode. The method the code gets on the system can be many and unpredictable. A download is a simple example for a proof-of-concept, but other possibilities include remote code execution via a browser, a "trusted" download becoming infected and other Windows security vulnerabilities.

This is a security flaw not because of how it is executed, but how the security system is designed. A prison where a prisoner can turn off the entire prison without tripping an alarm is a bad prison.

February 1, 2009 at 10:06 am

@Long Zheng: Ok, I understand now. But you are talking about automating keystrokes. Couldn't far more damage be done with enough

agcd07

keystrokes, UAC aside? The keystroke automation thing can be applied to hundreds of different things. Maybe MS should think about how easily keystroke automation can take advantage of things.

February 1, 2009 at 10:11 am

★Long Zheng

@agcd07: Keystroke automation has its uses. This UAC flaw however is more important than anything else because once UAC is disabled, everything else can be manipulated without keystroke automation by a full-privileged malicious application.

February 1, 2009 at 8:35 pm

Leo Davidson

The UAC whitelist is anti-competitive, as well as being badly designed/secured.

Users cannot add 3rd party components that they use & trust to the UAC whitelist. Only Microsoft's own components can be on it. So, for example, third party file managers have to display at least one UAC prompt to get admin access while Microsoft's Explorer does not. That isn't an even playing field.

Similarly, users cannot remove Microsoft's components from the UAC whitelist. So if you do not use Explorer but do want the whitelist (which is on by default), you are forced to leave the security hole open for Explorer even though it doesn't benefit from you. Explorer's UI isn't isolated like an admin process is — its windows have "medium integrity" — so there doesn't seem to be anything to stop it being remote-controlled via mouse & keyboard events. (As the VBScript in the root post proves!) Which is an okay trade-off if you use it but a stupid security hole if you don't. (And it seems stupid for the UAC control panel itself to be on the whitelist.)

Sadly for me (a file manager nut), people don't seem to care much about anti-competitive behaviour that affects anything other than web browsers, so nobody AFAIK has picked up this story, although I did mail a bunch of sites about it.

More details here, including a confirmation from Microsoft:

http://www.pretentiousname.com/misc/win7_uac_whitelist.html

February 2, 2009 at 8:39 pm

asf

@Leo Davidson: I'm with you all the way on this. They do the same thing with MSI, use MSI or no logo for you, I don't understand how they get away with it.

February 3, 2009 at 12:53 am

Bryant

@asf

They get away with it because it's their OS. If you have a problem with it, buy a Mac (keep in mind that Apple is considering similar measures now that Mac marketshare is increasing after seeing how successful "approved applications" can be through the app store) or use Linux.

As for Leo Davidson's post, I disagree with most of the FUDmongering except for the bit about explorer having unlimited admin access while holding medium integrity. That's definitely a design flaw.

February 3, 2009 at 4:42 am

Leo Davidson

@Bryant,

What, exactly, was "FUDmongering" about my post? Everything in it is a verifiable fact and the inability to change the whitelist confirmed by MS.

And how, exactly, would switching to another platform solve my problem when you yourself say the vendor of that platform can be even worse than Microsoft and when it doesn't run the apps I want to run?

You're using the idiotic "if you don't like it then move" argument. Please don't do that. I like Windows in general, but not this particular aspect of

Windows 7. If I didn't like Windows and wanted to use OS X or Linux then I wouldn't bother raiing issues about it. I Windows to be as good as possible. I want Microsoft to give the user control over their machine and give developers a level playing field. If your answer to every possible problem is "go use something else" then you will quickly run out of things to use.

As for "because it's their OS" you may have heard of the anti-trust trials in both the USA and the EU which say that just because it's their OS does not mean they are allowed to give special treatment and backdoor APIs to their applications.

February 3, 2009 at 5:21 am

DK

This is a stupid post. If you have a malware running under Administrator privileges on your machine, changing UAC would be the last thing it would do, after copying your files to an unknown ftp site in China, tapping into your keyboard strokes for credit card and other info, copying off any passwords to the remote site and formatting your hard disks. I guess you are not too worried about all that I guess.

Get a life dude, if you have a trojan running under Admin previleges on your machine, it is GAME OVER. (Of course you cannot get cheap popularity by overblowing things)

February 3, 2009 at 5:51 am

Leo Davidson

@DK, the point is that UAC is supposed to prevent things from running with admin privileges but, by default on Windows 7, there is nothing to stop something without admin privileges from turning off UAC (if you are logged in as an admin, which is what UAC Is supposed to allow us to do without giving all apps admin privileges).

It's annoying that so many people don't even grasp what UAC does yet feel the need to bash the root post with such strong statements.

February 3, 2009 at 6:05 am

Don

OK guys, it's one thing to keep on arguing about the implementation details of all this. I can boil down my issue with this down to something real simple. The default UAC setting on a freshly installed Windows 7 beta machine reads:

"Notify me only when programs try to make changes to my computer."

Rafael's VB script, which is a program, is able to circumvent the notifications that this default setting claims I will receive.

Now if everything really is by design as Microsoft say, then perhaps the text above needs to be modified to be more clear on what the policy actually means.

February 3, 2009 at 9:56 am

★Long Zheng

@DK: I thought you'd know better for someone working at Microsoft, if you had read the post correctly you'd know the malicious code is running in with **standard user privileges** and would be able to turn off UAC.

February 3, 2009 at 4:55 pm

Chris Lees

@ Todd Joley: It's a case of the pot calling the kettle black. The Windows 7 flaw allows a running program to silently turn off UAC. There was a Mac OS X flaw since the very beginning that allowed a running program to silently gain root access and, if it wanted, turn off OS X's sudo functionality as well. This depended on the presence of a setuid Cocoa program (the entire exploit was a single line of Applescript). When Apple shipped Tiger, it came with a setuid Cocoa program that could be exploited – ARDAgent. Apple was warned 4 years ago of the potential problem by one of its own security consultants, but ignored the problem until August 2008.

If the malicious Windows 7 program is run under a limited-only user account, UAC kicks in to stop the malicious program. The OS X exploit

ran successfully under a limited-only user account.

So, before you criticise Microsoft for badly engineering their operating system, take a look at Apple's history. The website http://www.rixstep.com has a lot of information about security flaws and potential data loss problems that are still present in OS X.

February 3, 2009 at 5:24 pm

Richard Wooding

Perhaps Microsoft should look at the Linux equivalent of UAC. Much less annoying but provides the same level of protections.

February 3, 2009 at 10:33 pm

REM

It's a release candidate so they will change very little. I tried to ask and have stuff changed when I beta testing Vista and they would not change anything.
Don't get your hops to high. This is just a remake of the almighty Vista.

This is why I no longer use Microsoft products and only Linux.

February 3, 2009 at 10:54 pm

Good_Bytes

What is sad but true, is I think that Windows Vista 64-bit (not 32) [NT 6.0] is actually better than Windows 7 [NT 6.1]. Like Windows 2000 (NT 5) was better than XP (NT 5.1). Sure, you have less features, and that the kernel and many other things are less optimized, but security wise and usability (maximize windows boarder and superbar doesn't change to opaque and dark colored) and more and indeed better. And I think I can live without Aero snap and teh superbar.. I mean I lived without them since Windows 3.1 and DOS times.

To say the truth if RC of win7 doesn't change a lot of things, I might stay with Vista and perhaps change to Win8.

Well who knows maybe Win7 SP2 will save it. :rolleyes:

February 3, 2009 at 10:56 pm

Damn

I havent seen such a holy shit like this 😕
Try doing some agriculture business :), it better suits you

February 4, 2009 at 6:03 pm

Patrick

Dear Long,

Could you please email me regarding another UAC flaw. I would prefer not to detail it on your site at this stage.

Regards,

Patrick

February 6, 2009 at 7:26 am

Andrew

Good grief can't Microsoft fix this whole least-privilege issue yet? Mainframes have been doing it since, what, 1965 or something. Letting the users play with the OS is a good way to ensure the computer won't work when you need it. Having only a single privileged user was OK on toy computers before anything was networked, but that was 30 years ago.

I was glad to see that the "user accounts" page recommends a standard account, and no longer calls it "limited" like in XP. But the "keep-clicking-OK" install only gives you a single administrator account. Duh.

"free malware protection" – ever heard of zero-day exploits ? Antivirus only protects against old vulnerabilities (though, yes, those can be quite enough to enable conficker or whatever)

"Perhaps Microsoft should look at the Linux equivalent of UAC. Much less annoying.." – if that's SELinux, I disagree (that it's not annoying). It

isn't turned on for most stuff yet. Try running an antivirus email filter, or a webserver that isn't bog-standard Apache running off the lone system disk.. Same thing – turn it off or go insane trying to write rules or get RedHat to patch the official version.

Running unprivilileged is such an effective, free, and generally easy defence against malware, viruses and general stupidity that it ought to be the out-of-box standard. Letting malware change your privilege level negates the whole point of doing it in the first place – it is a privilege-escalation exploit., and needs to be fixed as the serious security bug that it is.

February 10, 2009 at 10:47 am

Pat

Naive people should stick with a Mac or Leapfrog. They're limited and pretty.
People don't write viruses or malware for platforms that aren't widely adopted.
Don't run programs you don't know the origin AND function of.
Don't get mad at companies because they listened to your complaint when you cried wolf on UAC the first time and ignore you when you admit you were wrong in the first place. They know no matter what they do you'll complain.

April 25, 2011 at 1:36 pm

Brian

There is a huge difference between having every single minor thing pop up a UAC alert and allowing any program to alter the UAC level without ever notifying the user or asking for their permission. In the case of the UAC they DID NOT listen. If they had listened they would still have had a strong security concept included in it but given users/administrators a way to exempt or always allow specific programs prevent the constant pop ups which nullify any positive affect the UAC offers. That is on top of the fact that they apparently purposefully created this security hole which in no way is related to the original complaints. I do not remember anyone ever complaining that you received UAC notification when changing the UAC level.

So according to you everyone needs to program and compile all of the programs that they use on their computer, because that is the only true way you can really know the origin and function of the program. If the bad guys wanted to they could create and provide install material that appears to be as legit as anything you get from a real company, which means only when a person created the program themself can they know what it does and where it came from.

There was no crying wolf. There were legitimate complaints from all users that the UAC popups were occuring too often when there was no reason for them to occur. There is no reason that a person should have 2-3 additional clicks just to start a game or other program that must have admin privledges in order to run. Also, as I stated above, no one ever said that MS should remove the UAC prompts when changing the UAC level.

April 6, 2009 at 1:57 pm

Why don't they remove the certificate from the UAC windows setting?

Wes

December 14, 2009 at 6:23 am

Anthony

Really your POC shows one thing. To an unintelligent user, it would be very easy to get infected. Some very basic firewall software would all but mitigate this risk. Your POC would be like leaving your keys on a table in a locked house, its still secure. Really if your a big enough idiot to download every piece of maleware and bloatware you find across the internet you deserve what you get hit by. This is only a virus to unintelligible neanderthals, and gratz for spreading a plague of fear about a new operating system. All systems, security and software come with a few bugs in it. A setting you have to change to make it flawed, is hardly a loophole… Really stop the panic attacks and compare the level of security flaws to previous releases, its honestly a fairly solid release for an operating system.

December 14, 2009 at 6:38 am

Anonymous

Your proof of concept just wow…. A vrius for stupid people OMGZ who cares really. I backup my data if someone administratively took over my computer (oh well). I would A.) Be able to backtrace very likely the source of it because im not idiotic enough to allow maleware etc. to download on my system, it would have to be a malicious (active) take over. If it did get trhough zomg reboot/reinstall 30 mins later you did What? (nothing). Id personally rather take the risk then have to deal with the annoying UAC, and at Best a virus that rewrites the MBR with 0's and requires a Full Flash ZOMG you sure as hell dont need to exploit the uac to pull that off from Win n – Win N + 1. Theres always security holes no matter how well written your software is. 99% of a good security system is tracking any immediate intrusions, trace, report, making logs, and restricting access from the security breach as quickly as possible. And the fact you would go ZOMG over someting as minor as this compared to some flaws in the past, in many other operating systems as well shows your ability to hack is little more then a script kiddie. You rely on decieving the user into downloading and execing it as well. A True flaw would be through programs like windows mail itself, and finding ways to auto exec a file, forcing data packets through an unsecured port, not sir, what you are griping about(a virus for stupid people).

July 19, 2010 at 10:32 pm

dE

Despite all Microsoft's nagging, you still all use windows. Besides UAC is a copy of Unix permissions which was implemented more than 50 years ago and always was better than this piecea crap.

July 19, 2010 at 11:34 pm

dE

Actually it's not working dude…

July 20, 2010 at 8:37 pm

Patrick

@dE: Actually I have “switched” across to Linux and I’m one of the posters from above. I have been a user of MS products from 95-2005 (i.e. 95 to XP). Not buying into Vista/7/Server 2008 etc. I think MS went on a big tangent with UAC – should have focused on getting users into (true) non-admin rather than attempting to “constrain” administrators.

January 17, 2011 at 8:14 am

JJM

Why do you think the word “Microsuck” has been added to the dictionary? Windows 7 is a mess for sure. The super annoying interface that feels like its looking over your shoulder at all times is easily hacked. I myself have put together simple scripts to rape the system. The bottom line is the same as it has been for every other Microsoft product out there(Internet Explorer anyone?). They are insecure. Nothing will replace a third party antivirus/firewall program. Its all you need. They can run silently and not bother you at all. Windows 7 settings are never user friendly. I HATE MICROSOFT. I alway have for a good reason. They ignore the consumer. Where I come from if you try to sell the consumer a product while at the same time flipping the bird, you don’t deserve to be in business. That’s the reality.

April 25, 2011 at 1:17 pm

Brian

I find it unfathomable that they would purposefully leave incredibly dangerous flaw in the system, but still refuse to allow us to intentionally choose and exclude programs from popping up the UAC. It is almost as if they would rather we turn it off and use 3rd party programs for it all.

May 12, 2011 at 9:56 pm

rahman

not so excited..

July 16, 2012 at 12:32 pm

Surging killer

The reason they did not fix the issue, is because Microsoft built a backdoor into windows 7 for future spy applications that without the security flaw in the UAC would activate the measure notifying users that the CIA is spying and collecting data on your system….. sources, Microsoft and the talk about the backdoor they deny making for the RSA and the huge CIA data/profiling/spying center the US government paid for with tax payers money, Everyone should know by now Microsoft cannot be trusted too keep your data safe, that is why they release a new operating system every year or 2 because people find the holes microsoft puts in their operating systems and when they run out of holes they have too make a new OS with new holes..

Comments are closed.

Long Zheng

User experience entrepreneur
Melbourne, Australia

I'm a person and stuff. Mostly person, sometimes stuff. Proud introvert.

I make/made stuff people love to use:
MyPal: unofficial Melbourne myki mobile app, Omny Studio: enterprise podcast hosting, PTVGlass: Melbourne bus, tram & train timetable on Google Glass, Map2Glass: type and send addresses to Google Glass, SoundGecko: text-to-speech web reader, ChevronWP7: Windows Phone community unlocking, MetroTwit: Twitter app for Windows, Speedo Plus: Windows Phone GPS app, Bing Image Archive: browse daily backgrounds and Windows UI Taskforce: crowdsourced bug tracker.

LinkedIn

Email