The Old New Thing

It rather involved being on the other side of this airtight hatchway: Creating problematic files in a directory that requires administrative access

12 Sep 2013 7:00 AM | 23

A security vulnerability report came in that said, "If you create a file with □specific name□ in □specific directory□, then □denial of service□ happens the next time somebody does □specific operation□, and the machine must be rebooted."

Yes, it's true that creating that specific file in the very specific directory can sow the seeds for a denial of service, and thanks for pointing that out, and we'll fix the problem, but this is not a security vulnerability because □specific directory□ is writable only by administrators.

In other words, in order to carry out this attack, you need to gain administrator privileges. But if you have administrator privileges, then you're already on the other side of the airtight hatchway. If your goal was to attack the machine by triggering a denial of service that forces a reboot, then just use your administrator privileges to shut down the computer! No need to go about this clever roundabout way of triggering a denial of service when you can take the direct approach.

It's like saying, "If you go to the master control panel and throw all the auxiliary switches, then the circuit breaker will trip, and the plant will shut down. This is a security vulnerability in the master control panel."

First of all, thanks for letting us know about the problem with the master control panel. We'll have our engineers look it. But the master control panel is in the control room, and you need security clearance to get into the control room in the first place. And if somebody with security clearance wants to shut down the plant, then instead of throwing all the auxiliary switches to trigger a shutdown, then can simply hit the *emergency shutdown* button.

Blog - Comment List MSDN TechNet

Comments

Joshua
12 Sep 2013 7:43 AM
#

Some virus trick used to be apply a bunch of these then patch them in RAM so that if you removed the virus your machine broke.

Rick C
12 Sep 2013 7:47 AM
#

Apparently browsers[1] other than IE don't like ⟨ and ⟩.

Chrome displays them as the hollow box glyph, and a quick search says that in the past

FF and Safari didn't render them properly either.

Raphael
12 Sep 2013 7:51 AM
#

Opera 12 deals fine with ☐ and ☐

Also, the emergency shutdown (especially the SCRAM) is often something that does not require security clearance.

R Samuel Klatchko
12 Sep 2013 8:35 AM
#

I'm viewing this on Chrome and see ☐ and ☐ fine. Double check the font you are using has glyphs for those.

Bob
12 Sep 2013 8:48 AM
#

Usually I agree with these analyses, but this time I see two possible differences....

Creating the file may not be logged, while shutting down the machine is. So, if there are multiple administrators, one loses non-reputability.

Also, shutdown would require the re-entry of the administrator password. So, if the person sits down at an open console without knowing the password, they perhaps couldn't do a normal shutdown, but could create such a file.

So, it is good that Microsoft fixed the vulnerability.

> [*If you have multiple administrators, you already lose non-reputability. The rogue administrator can falsify the logs. And if you find an open console, you can just type "shutdown -t 0", no need to re-enter the password.-Raymond]*

alegr1
12 Sep 2013 10:10 AM
#

@Bob:

"I found that an administrator can FUBAR the machine. Please fix that"

"Thanks for noticing that. We'll do that, only if you'd be so kind to send us the solution to the halting problem".

JJJ
12 Sep 2013 10:20 AM
#

@Bob: You're not making the system any more secure by fixing this bug. How about for a denial of service on an already-open admin console, you just delete the database that runs your company? Or wipe user home directories? Or download a malicious trojan and replace admin utilities with it? Or install a keylogger?

A denial of service that forces a reboot is probably the most benign thing you can do...

You're doing exactly what the original "vulnerability" reporter did: focusing on a single tree in an infinite forest of malicious acts.

morlamweb
12 Sep 2013 10:24 AM
#

In my office, all of the circuit breaker panels are locked, so the analogy would be a little different: "if I open the breaker panel and open all of the auxillary switches, ..." "Well, if your goal is to shut off power, then why don't you just open the master breaker switch in the panel?" The security vulnerability isn't in that one file causing a denial of service; the vulnerability would be if a non-privileged user had the ability to write that file. According to Raymond's post, they don't, so it doesn't pass the test as a security problem.

@Bob: yes, the act of writing a log file likely wouldn't be logged (NTFS auditing is almost certainly off for that "special file") and shutdowns are logged, but that doesn't matter. You still need to be an Admin to pull it off. And if a bad actor has admin rights, then they can simply erase the event logs!

dave
12 Sep 2013 1:03 PM
#

@bob:

>shutdown would require the re-entry of the administrator password.

Removal of the power cord is generally not password-protected.

And if you're very lucky and you remove the power cord at precisely the wrong moment, you can deny even more service while the file system gets rebuilt.

Joshua
12 Sep 2013 1:05 PM
#

[If you have multiple administrators, you already lose non-reputability. The rogue

administrator can falsify the logs.]

That's what rsyslog is for. Last I checked (NT4), the Windows event log could be cloned to a listening rsyslogd.

ErikF
12 Sep 2013 1:10 PM
#

Easy fix for that: unplug the network cable (or it's moral equivalent, unbind the interfaces.) If you're an admin, there is basically nothing that can stop you if you're determined enough!

ErikF
12 Sep 2013 1:11 PM
#

Or, of course, just disable the service. Admins can do that too.

Kirby FC
12 Sep 2013 1:46 PM
#

Rick C

Apparently browsers[1] other than IE don't like ☐ and ☐

Apparently Firefox renders ☐ and ☐ as parenthesis instead of angled brackets.

Matteo Italia
12 Sep 2013 3:35 PM
#

[Apparently Firefox renders ☐ and ☐ as parenthesis instead of angled brackets.]

I see them just fine in FF 23.

Entegy
12 Sep 2013 6:36 PM
#

I see the proper character (FF26, woo Nightly!) here too.

iWantSimpleLife
12 Sep 2013 6:58 PM
#

If you are in the vault of a bank, you can easily take the money there and put it in your pocket. There are no security guards standing in the vault to guard the money (Although there are guards outside). This is a security issue, there should be security guards within the vault itself to prevent people from taking the money. Woot!

Engywuck
12 Sep 2013 11:00 PM
#

Well, there's a difference between "security vulnerability" and "having admin access". For example there exist designs for nuclear power stations where even the operators at the main console cannot force the station into an unsafe mode. The idea being that if it cannot be forced to do so accidents that do so can't happen either (and terrorists cannot do so, etc).

But of course even in these systems, a rogue "admin" could force the power distributed from the system to go offline - just break some cables :-)

Rick C
13 Sep 2013 8:07 AM
#

It's a mystery about the angles, I guess. I'm using Windows 8 x64 and whatever the current version of Chrome is, and whatever it's default font is: I don't normally mess with such things. Dunno why it's not working but it's not a big deal, except that by default IE gets it right.

Rick C
13 Sep 2013 8:14 AM
#

Weird. I tried fiddling with the fonts, and nothing. I copied a block of text with the angles and pasting into Word and the angles showed up. Fiddling with the encoding in Chrome did nothing--it just doesn't want to display them.

PW
13 Sep 2013 10:01 AM
#

I'd argue it could definitely be considered vulnerability, depending on the details. For example, if a seemingly innocuous action results in someone without admin privileges being able to trigger a DOS at a time of their choosing, especially remotely.

I may be able to trick an admin into allowing a file to be written somewhere that looks rather innocent, and then trigger the exploit at an opportune moment. The odds of being able to trick an admin into triggering a reboot at exactly the right moment are much smaller.

alegr1
13 Sep 2013 10:47 AM
#

Well, here is a hair-raising story of a major corporate product of a major corporation (the one where programs go to die).

It has a DLL in %TEMP%. If the DLL is missing, it will be automatically restored on next reboot. The DLL is persistently loaded in a process of that product. The DLL's file description says "Run-time Garbage Collector". It doesn't seem to be checked for integrity. You can tweak its ACL, though, to prevent it from loading.

If that's not a vulnerability, I don't know what is.

DWalker
13 Sep 2013 11:07 AM
#

@morlamweb:

"In my office, all of the circuit breaker panels are locked, ..."

In most jurisdictions in the US, I think that is a violation of Fire Department rules. The local Fire Department comes in and looks around every once in a while, and they make sure the exit signs are all illuminated, etc. Once they told us we can't store any boxes or anything else on the floor in front of the circuit breaker panels, because it impedes access if anyone wants to throw the breakers.

morlamweb
13 Sep 2013 12:40 PM
#

@DWalker: Well, you'd better tell the facilities dept to go remove the locks on all of the panels (including the ones for critical equipment that must be powered on 24x7x365!!) leaving them open for abuse by employees/contractors/guests/etc. Oh, and you'd better tell the manufacturers of said panels to stop making them because the locks "might be" in violation of fire codes. While I agree with you (and by extension, your local FD inspector) about storing things in front of the panels, there's a big difference between that and locks. In an emergency, it's relatively easy to break the lock on a panel (or have someone unlock it); it's not so easy to move filing cabinets, heavy boxes, whatever out of the way to to get to the panel.