

Novell Client login form enables reading and writing from and to the clipboard of the logged-in user

Novell Client login form enables reading and writing from and to the clipboard of the logged-in user

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-05/msg00418.html>

- *From:* "EitanCaspi@xxxxxxxx" <eitancaspi@xxxxxxxx>
 - *Date:* Sun, 21 May 2006 23:51:51 +0200
-

Suggested Risk Level: Low.

Type of Risk: Information Leakage, Information Injection, Unauthorized Access.

Affected Software: Novell Client for Windows, versions 4.9 and 4.8 (On windows XP Pro and Windows 2000 Workstation).

This versions are the only one tested, thus other version may be vulnerable as well.

Local / Remote activation: Local.

Summary:

1. Anyone with access to the computer's local operating system console, one using the Novell client login screen (when the console is locked), can view a textual content of the clipboard of the locally logged in user, by performing a paste command into the "user name" field of the login form.

2. Anyone with access to the computer's local operating system console, one using the Novell client login screen (when the console is locked), can inject its own textual content into the clipboard of the currently logged-in user by adding, temporally, a text string into the "user name" field of the login form, and then copy it into the clipboard.

This can also be done if no user is yet logged-in to the computer (after booting the computer or after a user logged off).

The text will remain in the clipboard after a user logged in, and if the user will perform a paste command the content will be injected into the user's console session.

Summary Notes:

Novell Client login form enables reading and writing from and to the clipboard of the logged-in user1

Novell Client login form enables reading and writing from and to the clipboard of the logged-in user

1. One must remember that access to the console may be achieved not only by a local presence of the attacker but also via a remote control application, if one is installed on the computer.
2. I assume non-textual content is accessible as well, but due to the nature of the relevant field in the login form only textual content can be pasted into it.

Possible Abuses:

1. A local attacker can read the last textual information added to the clipboard by the logged in user, without a need to authenticate.
2.
 - A. A local attacker can damage the logged in user's data if a careless user will paste the attacker's text into any application, and the user will not review it before using it.
 - B. A local attacker can damage the logged in user's operating system or applications if a careless user will paste the attacker's text as a command, and the user will not review it before executing it.

Reproduction:

1. Clipboard read:

- a. Log in to the operating system.
- b. Open any text editor (or any textual field in the operating system or application), and write a unique text.
- c. Copy the text you just wrote (select it and press ctrl+c).
- d. Lock the console by pressing ctrl+alt+del and clicking on the "lock computer" button.
- e. Press ctrl+alt+del to open the Novell login form.
- f. Click in the "user name" field and if there is a text inside, delete it or select all of it.
- g. Press ctrl+v, and the text you copied before will appear in "user name" field.

1. Clipboard write:

- a. Log in to the operating system.
- b. Lock the console by pressing ctrl+alt+del and clicking on the "lock computer" button.
- c. Press ctrl+alt+del to open the Novell login form.
- d. Click in the "user name" field and if there is a text inside, delete it or select all of it.
- e. Write a unique text.
- f. Copy the text you just wrote (select it and press ctrl+c).
- g. Delete this unique text.
- h. Perform a regular log in to the operating system.
- i. Open any text editor (or any textual field in the operating system or application), and press ctrl+v, and the text you copied before will appear.

Steps "a" and "b" can be replaced by booting or restarting the operating system and once the graphical interface has been displayed, proceed to step c.

Novell Client login form enables reading and writing from and to the clipboard of the logged-in user

Exploit Code: No need.

Direct resolution: None at the time this advisory was published.

Workarounds:

WARNING: The following listed applications are not made by me and I have no knowledge if they will perform as expected and if they will not damage your hardware and/or software. Using this applications is totally at your own risk and responsibility.

I only mention this applications in this advisory as possible workarounds to overcome the vulnerability mentioned in this advisory.

Following are some freeware applications intended to clear the clipboard. Some of the applications can be activated manually (before locking or leaving the desktop) and/or some of the applications can be initiated via a command line, which makes them suitable to be scheduled by the windows tasks scheduler to run every X minutes/hours or run while the operating system is idle.

AutoClipClear

http://www.geocities.com/visualfantasy_studio/acc.htm

It has no interface nor settings to adjust. Can be run in via a command line.

NirCmd

<http://www.nirsoft.net/utills/nircmd.html>

It has only textual interface but many extra functions (one of them is locking the console, so one can make a batch file to clear the clipboard and then lock the console). Can be run in via a command line.

ClipClear

<http://www.moonsoftware.com/freeware.asp#clipclear>

It has a task bar icon and clicking it clears the clipboard. I guess it will not be suitable to run as a scheduled task since activating it only makes it available at the task bar. It has no startup switches.

I tried to find a scheduler that can run an application at the event when the workstation is being locked, but found only this two:

1. Funny, but someone asked just that at Novell's site and he was answered that this can be done with NALRUN32 and NALRUNW from Novell's "Workstation Manager" ("ZEN 2 Application Management Tool Kit"), but without a proper example.

<http://www.novell.com/coololutions/qna/4332.html>

http://www.novell.com/coololutions/zenworks/features/a_zen2_toolkit_zw.html

#nalrun

2. The task scheduler of windows vista will be able to do this (when windows vista will be officially released...).

Novell Client login form enables reading and writing from and to the clipboard of the logged-in user3

Novell Client login form enables reading and writing from and to the clipboard of the logged-in user

<http://www.microsoft.com/technet/windowsvista/mgmntops/taskschd.mspix>

Vendor Notification: Novell was notified of this issue more than two months ago.

Due to my feeling that the company was not acting to solve this issue, I notified them after one month, that I will wait another month, and if at that time the company will not publish an advisory and/or a patch I will publish my own advisory.

Since the company did not publicly acted regarding this vulnerability within this time frame, which I think is reasonable this advisory is now published.

Novell's lack of action may be due to the low risk nature of this vulnerability.

Credit:

Eitan Caspi

Israel

Email: eitancaspi@xxxxxxxxx

Past security advisories:

1.

<http://online.securityfocus.com/bid/4053>

<http://www.microsoft.com/technet/security/bulletin/MS02-003.mspix>

<http://support.microsoft.com/default.aspx?scid=KB:en-us;315085>

2.

<http://online.securityfocus.com/bid/5972>

<http://support.microsoft.com/default.aspx?scid=kb:en-us;Q329350>

3.

<http://online.securityfocus.com/bid/6280>

<http://www.securityfocus.com/archive/1/301624>

4.

<http://online.securityfocus.com/bid/6736>

<http://online.securityfocus.com/archive/1/309442>

5.

<http://www.securityfocus.com/bid/7046>

<http://www.securityfocus.com/archive/1/314361>

6.

<http://www.securityfocus.com/archive/1/393800>

<http://service1.symantec.com/SUPPORT/ent-security.nsf/3d2a1f71c5a003348525680f006426be/c937e09a6ad4e20688256a22002724bb?OpenDocument>

Novell Client login form enables reading and writing from and to the clipboard of the logged-in user4

Novell Client login form enables reading and writing from and to the clipboard of the logged-in user

Articles:

You can find some articles I have written at

<http://www.themarker.com/eng/archive/one.jhtml>

(filter: Author = Eitan Caspi (second name set), From year = 2000 , Until year = 2002)

Eitan Caspi

Israel

Professional Blog (Hebrew): <http://www.notes.co.il/eitan>

Personal Blog (Hebrew): <http://blog.tapuz.co.il/eitancaspi>

Blog (English): <http://eitancaspi.blogspot.com>

"Technology is like sex. No Hands On – No Fun." (Eitan Caspi)