

RE: Fwd: Terminal services and remote programs.

RE: Fwd: Terminal services and remote programs.

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2008-05/msg00040.html>

- *From:* "Shenk, Jerry A" <jshenk@xxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 5 May 2008 17:48:13 -0400
-

Much of the exploitability of a Citrix or Terminal services type solution relates to how the application works. I audited a site where multiple companies shared a common front end. The security of the data relied on that front end. In this case, I was able to use the "help/about vulnerabilities" that were mentioned here a few days ago. The bulk of the discussion here has been on the ability to escalate privileges for an authenticated user but, in WAY TOO MANY cases, escalation isn't even necessary.

-----Original Message-----

From: listbounce@xxxxxxxxxxxxxxxxxx [mailto:listbounce@xxxxxxxxxxxxxxxxxx]
On Behalf Of Sat Jagat Singh
Sent: Monday, May 05, 2008 1:43 PM
To: PenTest
Subject: RE: Fwd: Terminal services and remote programs.

I'll count myself as corrected on the issue of privilege escalation through MS Office. I actually did find one. MS06-009 pertains to a vulnerability in the Korean Input Method Editor of multi-language versions of Office 2003 that Microsoft says can be exploited to escalate privileges. So, that's pretty obscure and unlikely to be found in most environments. But it demonstrates that such a thing is conceptually possible.

Concerning access control and other "unauthorized" access, in some environments simply being able to use ping or browse the network is a violation of policy, though it may not violate the configured access rights. One needs to distinguish between what is authorized in the sense of managerial policy versus permissions that are actually configured. These types of unintended access are often the gateway to finding poorly secured assets that are actually sensitive. That is why such desktop restrictions are implemented as one way of enforcing access control. You are certainly correct that in and of themselves these measures are not access control.

--- On Fri, 5/2/08, Thor (Hammer of God) <thor@xxxxxxxxxxxxxxxxxx> wrote:

RE: Fwd: Terminal services and remote programs.

RE: Fwd: Terminal services and remote programs.

From: Thor (Hammer of God) <thor@xxxxxxxxxxxxxxxx>
Subject: RE: Fwd: Terminal services and remote programs.
To: "PenTest" <pen-test@xxxxxxxxxxxxxxxx>
Date: Friday, May 2, 2008, 3:50 PM
Inline:

-----Original Message-----
From: listbounce@xxxxxxxxxxxx