

# [NT] 2X ThinClientServer Create Admin Account Replay Vulnerability

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-12/msg00018.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxxx)>
  - *Date:* 19 Dec 2006 09:55:20 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>  
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

## 2X ThinClientServer Create Admin Account Replay Vulnerability

---

### SUMMARY

2X ThinClientServer provides "a complete solution for the central deployment, configuration and management of thin clients, and provides load balancing and redundancy of terminal servers". It is possible to create administrative user accounts for the application, without authentication.

### DETAILS

During the installation procedure, an administrative user account for the application is created. Sending the same request with a different username, after the installation is completed, creates an additional administrative account. The account can be created remotely and authentication is not required.

#### Vendor Response:

The above vulnerability is fixed and applicable to the following versions:

- ThinClientServer 4.0 – Users of ThinClientServer Version 4 are unaffected by this issue.
- ThinClientServer 3.0 – Please Upgrade your machine to Version 4.0.2248

[NT] 2X ThinClientServer Create Admin Account Replay Vulnerability

or higher and deploy the new ThinClientOS 4.0 on your network to resolve this issue. This can be done by uploading the new image zip file in the Management Console and setting it as the new default image for your ThinClients.

Customers who have prior versions of ThinClientServer are requested to upgrade to at least 4.0.2248 version.

Recommendation:

Upgrade to Version 4.0.2248 or higher to solve the issue.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6221>>  
CVE-2006-6221

ADDITIONAL INFORMATION

The information has been provided by <[mailto:oliver\\_karow@xxxxxxxxxxxxxx](mailto:oliver_karow@xxxxxxxxxxxxxx)>  
Oliver Karow.

The original article can be found at:

<<http://www.symantec.com/enterprise/research/SYMSA-2006-012.txt>>  
<http://www.symantec.com/enterprise/research/SYMSA-2006-012.txt>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

[list-unsubscribe@xxxxxxxxxxxxxx](mailto:list-unsubscribe@xxxxxxxxxxxxxx)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@xxxxxxxxxxxxxx](mailto:list-subscribe@xxxxxxxxxxxxxx)

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.