

[NEWS] Security Issue with GroupWise and LDAP Authentication in PostOffice (Anonymous bind)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-03/0010.html>

From: support@securiteam.com

Date: 03/03/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sun, 3 Mar 2002 21:11:29 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Security Issue with GroupWise and LDAP Authentication in PostOffice
(Anonymous bind)

SUMMARY

A security vulnerability in the way GroupWise relies on the LDAP for authentication allows remote attackers to logon as any user they desire without requiring them to know its password. This is caused by inadequate checks to what type of LDAP binding has occurred (Anonymous, or Username Password based).

DETAILS

Environment:

GroupWise 6 Post Office using LDAP authentication AND security configuration of PostOffice leaves LDAP User Name and Password fields blank in the Post Office Agent object in ConsoleOne.

Exploit:

Run GroupWise as any user (either "grpwise /@u-?") or if you are not NDS authenticated, whatever the registry has stored as the last person who logged into GroupWise) and leave the password blank. Hit enter a couple of times and you will get right into the account.

Securiteam: [NEWS] Security Issue with GroupWise and LDAP Authentication in PostOffice (Anonymous bind)

Fix:

A. Novell has developed a workaround to this issue in the LDAP spec to prevent GroupWise accounts from being accessed without a password. This fix is found in the Field Test File FGW62N4.EXE. This can be found at support.novell.com and searching for the filename.

Pro: solves problem, retains current password functionality.

Con: New code comes with possible stability issues.

B. Without implementing the new code, the issue can be resolved as follows: Fill in the LDAP User Name and Password fields in the Post Office Agent object in ConsoleOne. The LDAP User Name is the eDirectory account that the POA, the Internet Agent, and the WebAccess Agent can use to log in to the LDAP server in order to authenticate GroupWise users.

Pro: This approach to LDAP authentication is faster and requires fewer connections to the LDAP server than if each GroupWise user authenticates to the LDAP server individually.

Con: From within GroupWise, users will not be able to use grace logins, nor will they be able to change their LDAP passwords.

Technical details (in Novell's words):

This is not technically a bug, but a configuration issue. In accordance with the LDAP v3 RFC 2251, an LDAP bind in which a username is provided but a password is not [i.e. blank] is treated as an anonymous bind.

This means that a bind is granted to users providing a username but no password. The bind granted is an anonymous bind but based on limitations in the LDAP specification, most LDAP implementations do not provide any indication that the bind is in fact anonymous. GroupWise relies on the success or failure of a bind to determine whether a users username and password is authentic when LDAP authentication is being used [if you put LDAP trace on you will see that blank password become anonymous binds]. The problem is in the RFC, not GroupWise. Once we realized that RFC had the hole, we made a change in the POA. This problem only came to our attention about 2 weeks ago so it takes time for information to get out.

ADDITIONAL INFORMATION

The information has been provided by <mailto:frnkblk@iname.com> Frank Bulk.

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

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.

- ***Previous message:*** support@securiteam.com: "[\[UNIX\] Avenger's News System Command Execution Vulnerability](#)"
- ***Messages sorted by:*** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)