

# [Full-Disclosure] NOVL-2005-10096251 GroupWise WebAccess error handling modules (report)

**Source:** <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-01/0771.html>

---

**From:** Ed Reed ([ereed\\_at\\_novell.com](mailto:ereed_at_novell.com))

**Date:** 01/21/05

Date: Fri, 21 Jan 2005 12:37:51 -0700  
To: "Secure Secure" <[Secure@novell.com](mailto:Secure@novell.com)>

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

For Immediate Disclosure

===== Summary =====

Security Alert: NOVL-2005-10096251  
Title: GroupWise WebAccess Error modules loading (report)  
Date: 21-January-2005  
Revision: Original  
Product Name: GroupWise 6.5, GroupWise 6.5 WebAccess  
OS/Platform(s): NetWare, Windows, Linux  
Reference URL: <http://support.novell.com/servlet/tidfinder/10096251>  
Vendor Name: Novell, Inc.  
Vendor URL: <http://www.novell.com>  
Security Alerts: <http://support.novell.com/security-alerts>  
Affects: login.htt, about.htt  
Identifiers: BugTraq 387566 -  
<http://www.securityfocus.com/archive/1/387566>  
Credits: Marc Ruef <[maru@scip.ch](mailto:maru@scip.ch)>, but thanks, too, to  
Pete Connolly <[pete@connolly.btinternet.com](mailto:pete@connolly.btinternet.com)> for  
actually notifying Novell's security team

===== Description =====

By specifying a query string (?error=<value>, or ?merge=<value>) on the WebAccess login URL (for example <http://webacc.company.com/servlet/webacc?merge=about>), an unauthenticated user is able get read-only access to various public templates and informational files, including the "about" page for the WebAccess server which includes the version of GroupWise that is installed.

===== Impact =====

The server is not granting access to private files, and no files can be modified through this attack. The "about" page which contains the version of the GroupWise software installed is available, however, it is not considered restricted information, since this same information is available on the normal login URL page.

Customers that are concerned about the version information being made public can edit login.htm and about.htm template files to remove this information. These templates are located in the following default locations:

NetWare –

sys:\tomcat\4\webapps\ROOT\WEB-INF\classes\com\novell\webaccess\templates\frames

Linux –

/var/opt/novell/gw/WEB-INF/classes/com/novell/webaccess/templates/frames

Windows –

C:\NOVELL\JAVA\SERVLETS\COM\NOVELL\WEBACCESS\TEMPLATES\FRAMES

Remove line 313 in login.htm and line 37 in about.htm.

Additionally, Novell will be making changes in the next update of GroupWise, version 6.5.4, to address these issues. The changes will be to ignore any query string parameters if the user is not authenticated.

Q. What files do non-authenticated users have access to?

A. Read only access to template files are allowed, which are stored in a public directory on the server, as well as a version file, which contains the version of the GroupWise software that is installed. There is no security risk in displaying the template files without data--the template files themselves do not contain confidential information. For the GroupWise 6.5.4 release, this will be addressed so that no unauthenticated users will be able to access any information other than the login page.

Q. What query strings expose this behavior?

A. The "error" query string and the "merge" query string can be used to access read-only versions of the WebAccess templates and the "about" information for the server. Note that there is no user data in these templates since the user is not authenticated. The merge query string works in the following way: when a user is logged in, actions that return data are performed. The resulting data is merged into the template specified by "merge" (or "error" if an error condition occurred) to produce useable output for the authenticated user. In the case where there is no authentication, there is no data to merge into the template. Authentication is not bypassed and there is no generic or "ghost" user logged in.

Q. What information or access is inappropriately divulged to unauthenticated users?

A. This approach offers no means for accessing restricted files on the server. If the version information about the server is deemed restricted, the administrator can edit the about.htm and login.htm template files to remove this information. These templates are located at template\frames on an installed WebAccess server.

Q. Is there any way for an attacker to write data into the server through this method?

A. The approach outlined provides no mechanism for modifying data or files on the server.

Q. Is it possible to use HTML injection to carry out a social engineering attack?

A. This supposition is false as the attack described has no ability to modify data or files on the server in order to inject malicious code into WebAccess pages.

===== Recommended Actions =====

See detailed instructions in the referenced Technical Information Document (TID) <http://support.novell.com/servlet/tidfinder/10096251>

===== DISCLAIMER =====

The content of this document is believed to be accurate at the time of publishing based on currently available information. However, the information is provided "AS IS" without any warranty or representation. Your use of the document constitutes acceptance of this disclaimer. Novell disclaims all warranties, express or implied, regarding this document, including the warranties of merchantability and fitness for a particular purpose. Novell is not liable for any direct, indirect, or consequential loss or damage arising from use of, or reliance on, this document or any security alert, even if Novell has been advised of the possibility of such damages and even if such damages are foreseeable.

===== Appendices =====

None

===== Contacting Novell Security Alerts =====

To report suspected security vulnerabilities in Novell products, send email to  
secure@novell.com

PGP users may send signed/encrypted information to us using our PGP key, available from the pgpkeys.mit.edu server, or our website at:

<http://support.novell.com/security-alerts>

Novell Security Alerts, Novell, Inc. <secure@novell.com>

PGP Key Fingerprint:

3C6B 3F26 4E34 1ADF E27B D6C4 1AC8 9184 34D1 9739 (revised)

=====  
===== Revision History =====

Original: 21-Jan-2005 - Original Publication

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.2.4 (GNU/Linux)

iD8DBQFB8U9JGsiRhDTRlzkRAj9xAJoCdB/5gaMtYh3vre9uDls76KsnngCg7PXz

AiVCn6GGHz4krUdAcgQkgrs=

=Hfuz

-----END PGP SIGNATURE-----

---

Full-Disclosure - We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>