

**Fix Release Notes**

Fix

Table of Contents

2. Introduction 2

3. Fix Details 2

4. List of Amended Files 2

5. Log No. Summary 3

# Introduction

This document defines the changes made to the product for Fix and is specifically targeted at end users.

After reading through this document, should you have any further training or consultancy requirements then please contact your Bentley account manager.

# Fix Details

|  |  |
| --- | --- |
| Fix Details Baseline Release |  |
| Fix Description | The fix applies fine-grain-access-control security on DOC\_LOCATIONS, HIG\_DIRECTORIES and DOCS |
| Prerequisites | Sole Access to the database tables and affected packages |
| Implementation Instructions | The staging folder is the location of the folder that .exe was extracted to (the folder containing this readme).  Log onto SQL\*Plus as the Highways Owner with the staging folder as the working directory.  At the prompt type START and press return.  Exit SQL\*Plus |
| Limitations |  |
| Configuration Information | None |
| How To Test | Recommend full regression test |
| Rollback Strategy | Initially implement on a test environment |

# List of Amended Files

|  |  |
| --- | --- |
| Filename | Version |
| Nm3nwausec.pkh | 1.5 |
| Nm3nwausec.pkb | 1.4 |
| Hig\_directory\_roles\_a\_iud\_trg.trg | 2.3 |
| Add\_nm3nwausec\_policies.sql | 1.4 |
| Drop\_nm3nwausec\_policies.sql | 1.1 |

# Log No. Summary

This chapter summarises all software issues that have been addressed by this fix.

For issues raised by customers, Bentley Technical Support Group (TSG) Ticket Numbers are cross referenced where applicable.

|  |  |  |
| --- | --- | --- |
| Details | Internal Reference | TSG Ticket Number |
| Securing of documents (see below) | S-92013  [TK-259862](http://versionone.bentley.com/VersionOne/Task.mvc/Summary?oidToken=Task%3A3114997) |  |
| Trigger failure on removal of a directory/role | D-121561 |  |

## Securing Documents

The document table until recently had no server-based security. It is used to hold records which relate to physical documents held inside one of various methods but also holds records that relate to public enquiries. This leads to the Documents table acting as two distinct partitions of data and each needs a separate restriction to secure the data.

Public enquiries carry an admin-unit which is denormalised from one of several sources such as the asset or road network to which it relates or from the admin-unit of the user who made the transaction that created the enquiry record. Admin-unit security was imposed on this table in a previous fix.

The task in hand is to impose further fine-grain-access-control to cover the security on the documents that relate to files.

The new security policy will apply purely to the document records that relate to files held within an Oracle directory mapped to an Exor HIG\_DIRECTORY through the existing role-based security. The original method stopped short of restricting the user from seeing the table data relating to these directories. This fix aims to secure the following Exor tables through the directory/role relationship:

* HIG\_DIRECTORIES
* DOC\_LOCATIONS
* DOCS

It does not affect any read/write/delete/execute privileges applied to these directories and it does not affect the security privileges on documents held as CLOBs inside an Oracle table nor those held on doc-locations which relate to middle-tier, FTP or other folders.

Predicates applied to these new tables will be applied through new policies and changes to the nm3nwausec package. Hence, the security fix is comprised of changes to the existing nm3nwausec package which was originally supplied in fix 1 and new scripts to add the new policies. During implementation of the fix, all the NM3NWAUSEC policies will be dropped and re-instated. A SQL script to drop the policies is also included. It is expected that the fix is applied whilst the tables are inactive and unavailable to other connections.

## Trigger failure on removal of a directory/role

A directory may be secured by a role and is a pointer to an Oracle directory which in turn, is a pointer to a file-system folder. Granting privileges to the directory/role will make an attempt to grant the permissions directly onto the file-system. However, the directory is an instance-wide Oracle object and the Exor HIG\_DIRECTORY is just a record in a table. Under some circumstances, such as after data import or in cases where the Oracle directory is dropped or if the file-system is modified, the link between the role and the file-system is broken. Under these circumstances, it may be relevant to drop the directory role. In the current release, this will automatically fail as the file-system permissions cannot be applied. The fix also includes the change to allow the removal of a directory role where the directory does not relate to a physical file-system location. Without the fix, under the circumstances such as those identified above, a failure will result as illustrated:

ORA-20000: HIG-0257: Object does not exist:

REVOKE READ ON DIRECTORY <directory> FROM <role>

ORA-06512: at "HIGHWAYS.HIG", line 1464

ORA-06512: at "HIGHWAYS.HIG\_DIRECTORIES\_API", line 467

ORA-06512: at "HIGHWAYS.HIG\_DIRECTORY\_ROLES\_A\_IUD\_TRG", line 48

ORA-04088: error during execution of trigger 'HIGHWAYS.HIG\_DIRECTORY\_ROLES\_A\_IUD\_TRG'

# Known Issues

This chapter gives a brief description of any other issues found during the development of the fix.

Internal references relate to defects held within the Bentley system. TSG ticket number may be added if the issue is known and has been raised by a customer otherwise the Ticket Number is remains unset.

|  |  |  |
| --- | --- | --- |
| Details | Internal Reference | TSG Ticket Number |
| MCI Bulk Upload form gives unhandled Java exception | D-121559 |  |
| Hig\_directories form HIG1895 gives unhandled Java exception | D-121560 |  |

## **MCI Bulk Upload form gives unhandled Java exception**

The MCI bulk download form starts with a default value derived from system or user option. The form needs a location which corresponds to an Oracle directory which is also mapped into a HIG\_DIRECTORY record. Each HIG\_DIRECTORY record may be associated with a role. If the user has no default directory (from the option), the location field is set to 'UNKNOWN'. The View Directory button is still active despite a meaningless location field. If used, the button attempts to read a non-existent directory. The result is an error message:

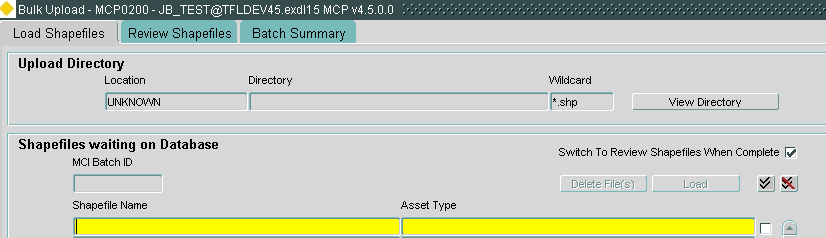
ORA-29532: Java call terminated by uncaught Java exception: java.lang.NullPointerException (raised in NM3FILE line 60).

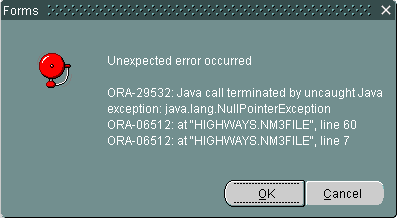
The same is true if the user has a valid location but this location has not been made available to the user through roles. In this case when the button is used, it will fail with the error :ORA-29532: Java call terminated by uncaught Java exception: java.security.AccessControlException:the Permission (java.io.FilePermission <folder> read has not been......

The form needs to de-activate the button in cases where the location is unknown or if the user has no privileges on the folder.

The imposition of the FGAC available in a 4.6.0.0 fix will prevent a user from seeing a folder on which they have no role-based permission. Hence, case 2 above will degenerate to case 1 after the fix has been applied.

Below are the screen shots displaying some of the outcomes that might arise.







## **Hig\_directories form HIG1895 gives unhandled Java exception**

The HIG\_DIRECTORIES form HIG1895 provides a list of Java Role Privs for each directory. Usres may set the Read/Write/Delete/Execute flags for each of the directoires. However, a subordinate user may not have access to the directory due to the role-based permissions. an attempt to set the privilege will fail if the user has not been configured with the dictionary access required. The failure is an unhandled Java exception such as ORA-29532 - Java call terminated by uncaught Java exception.....

Imposing FGAC on the direcrory will limit the occurrence of this since the user will only see the directories to which they have been given permission through the roles. Having the role does not give the user the right to set the properties of the access rights made available to the role.

