

Export

Peak Incident Management System

Call Reference	PC0225071	Call Logger	Andy Dunks -- Security Ops
Release	Targeted At -- HNG-X 09.28	Top Ref	AUDIT_EXTRACT_SVR_0928_D067-D066
Call Type	Live Incidents	Priority	A -- Business stopped
Contact	Andy Dunks	Call Status	Closed -- Administrative Response
Target Date	07/11/2013	Effort (Man Days)	3.00
Summary	Possibility of missing transactions on ARQ Audit spreadsheets		
All References	Type	Value	
	Clone Call	PC0225656	
	Product Baseline	AUDIT_EXTRACT_SVR_0928_V067	
	DevIntRel-Director	Live Supp.Test	
	Product Baseline	AUDIT_EXTRACT_CLT_0928_V082-V081	
	Product Baseline	AUDIT_EXTRACT_SVR_0928_D067-D066	
	Product Baseline	AUDIT_EXTRACT_SVR_0928_V067-V066	
	Product Baseline	AUDIT_EXTRACT_CLT_0928_V082	
	Product Baseline	AUDIT_EXTRACT_CLT_0928_D082-D081	
Collections	Name	User	Date
	RP-release_planning	Lorraine Guiblin	24-Apr-2013 14:36:44
Impact Statement	User	Date	
	Gerald Barnes	12-Jun-2013 15:59:13	
	There is a loop hole in the code of QueryDLL.dll where by if it is running during the evening service shutdown the resulting prosecution spreadsheets produced later may have missing transactions.		
	There is a tiny possibility that errors in the QueryManager service may not be reported meaning that invalid prosecution spreadsheets may be produced.		
	There is the possibility of errors being generated when audit queries are being run and the QueryManager service is shutdown and restarted. This wastes the time of the prosecution service and makes them rerun queries. This makes achieving SLAs more difficult.		

Progress Narrative

Date:16-Apr-2013 08:56:09 User:Andy Dunks

CALL PC0225071 opened

Details entered are:-

Summary:Possibility of missing transactions on ARQ Audit spreadsheets

Call Type:L

Call Priority:A

Target Release:HNG-X 08.00

Routed to:Audit-Dev - _Unassigned_

Date:16-Apr-2013 08:56:08 User:Andy Dunks

[Start of Response]

There is a small possibility of missing transactions on generated spreadsheets if the query handling was run during the evening Query Manager shutdown.

A flaw has recently been spotted in the audit code. It was introduced in the fix to PC0187097 quite some time ago (but post HNGx).

Passing call to Audit Dev as they have requested this call to be raised.

[End of Response]

Response code to call Live Incidents/Defects(L) as Potential Problem Identified(38)

Date:16-Apr-2013 10:22:04 User:Gerald Barnes

The Call record has been assigned to the Team Member: Gerald Barnes

Date:16-Apr-2013 10:34:10 User:Gerald Barnes

Target Date/Time updated: new value is 30/04/2013 08:56

Development Cost updated: new cost is 14 (Man Days)

[Start of Response]

The problem is principally because of a fix introduced by PC0187097. The following change -

```
if (cStatus == CRFIQueryRequest::E_ABSTRACT_FILES_OK || //Directories created ok
    cStatus == CRFIQueryRequest::E_CONCAT_FILES || //Abnormal Termination last time - Try again
    cStatus == CRFIQueryRequest::E_CONCAT_FILES_FAILED || //Failed last time - try again
    cStatus == CRFIQueryRequest::E_ABSTRACT_FILES_FAILED ) //SM - PC0187097
```

meant that an error code generated on shutdown in the previous section is masked and as a result the shutting down whilst looping through files would not be noticed.

However because of this problem a meeting was held yesterday attended by Gerald Barnes, Adam Spurgeon, Alan Holmes and Steve Goddard and the following points would be acted upon -

1. I contact the prosecution service and request them to raise an A priority PEAK on this issue.
2. I advise them that in future they should check their QueryHandler.log for any instance of the line ?Shutdown Signalled - Process terminating? and if one occurs they should rerun their query.
3. They should check all submitted ARQ evidence for ?Shutdown Signalled - Process terminating? and if one occurs rerun the query as a precaution and confirm the results are the same as submitted.
4. I should very thoroughly re-investigate why the line ?cStatus == CRFIQueryRequest::E_ABSTRACT_FILES_FAILED) //SM - PC0187097? was added to address the PEAK PC0187097. The line just dose not look right for me. What ever was being addressed by this PEAK needs to be done another way.
5. I go through the code changing any indications of the ethos that a shutdown results in a failure being reported to a shutdown results in a rerun after service start. I note that although this needs thorough testing it is a fairly safe change because already if the Query Manager code does not respond to the shutdown signal in a timely manner it is just terminated resulting in the same behaviour.
6. I go through the code trying to spot any other instances of failure results being overwritten without being properly reported first.

[End of Response]

Response code to call type L as Category 38 -- Pending -- Potential Problem Identified

Hours spent since call received: 1 hours

Date:16-Apr-2013 10:37:39 User:Gerald Barnes

A new Business Impact has been added:

There is a loop hole in the code of QueryDLL.dll where by if it is running during the evening service shutdown the resulting spreadsheets may have missing files.

Date:16-Apr-2013 10:38:54 User:Gerald Barnes

The Business Impact has been updated:

There is a loop hole in the code of QueryDLL.dll where by if it is running during the evening service shutdown the resulting prosecution spreadsheets produced later may have missing transactions.

Date:16-Apr-2013 10:39:34 User:Gerald Barnes

Product HNG-X Platforms -- Audit Server (ARC) (version unspecified) added.

Date:16-Apr-2013 11:04:19 User:Gerald Barnes

[Start of Response]

DEVELOPMENT IMPACT OF FIX:

SPECIFY THE HNG-X PLATFORMS IMPACTED:

The platform is specified and it is the audit server.

TECHNICAL SUMMARY:

A loop hole has been found in QueryDLL.dll where by if it is running during the evening shutdown of the QueryManager service the prosecution spread sheets produced later may have missing transactions.

In addition the design ethos at the moment of QueryDLL is that on shutdown a failure state is indicated. This is to be changed to there being a rerun of the query after shutdown which would have prevented this problem in the first place although there would still have been a problem if a genuine error rather than a shutdown had occurred prior to the faulty code which masked the earlier state.

As well as that and as a precaution the error handling of QueryDLL.dll is going to be looked at and improved.

LIST OF KNOWN DIMENSIONS DESIGN PARTS AFFECTED BY THE CHANGE:

AUDIT_EXTRACT_SVR

DEPENDENCIES:

There are no dependencies.

DEPLOYMENT DETAIL:

It is a file to be replaced when the QueryManager service is quiescent.

DEV EFFORT IN MANDAYS:

The work is about 10 days but because of possible interruptions we should allow 3 weeks elapsed.

IMPACT ON USER:

The prosecution spreadsheets will be more reliable after this fix is applied.

IMPACT ON OPERATIONS:

The prosecution spreadsheets will be more reliable after this fix is applied.

HAVE RELEVANT KELS BEEN CREATED OR UPDATED?

No KEL has been raised because it is intended that this problem will be fixed quickly and all members of the prosecution team has been informed.

IMPACT ON TEST:

A prosecution spreadsheet should be produced by slow ARQ and fast ARQ before the fix is applied and with no service shutdown of the QueryManager service. These should be produced again after the fix and confirmed as the same. In addition with the fix in place it should be confirmed that these same spreadsheets are produced after shutting down the QueryManager service and restarting it at various points in both the fast ARQ and slow ARQ.

RISKS (of releasing and of not releasing proposed fix):

If this fix is not done then there is a serious risk of a spreadsheet being produced with missing transactions.

LIST OF LIKELY DELIVERABLES:

QueryDLL.dll

[End of Response]

Response code to call type L as Category 55 -- Pending -- Live Fix Impact Supplied

Hours spent since call received: 1 hours

Date:16-Apr-2013 11:07:18 User:Gerald Barnes

The call Target Release has been moved to Proposed For -- HNG-X 07.22

Date:16-Apr-2013 11:10:50 User:Gerald Barnes

Action placed on Team:RelMngmntForum

Date:24-Apr-2013 14:36:44 User:Lorraine Guiblin

The call Target Release has been moved to Targeted At -- HNG-X 07.22

Date:24-Apr-2013 14:36:55 User:Lorraine Guiblin

Targeted in PTF as requested

Date:24-Apr-2013 14:36:58 User:Lorraine Guiblin

Action has been removed from the call

Date:02-May-2013 17:12:07 User:Gerald Barnes

Target Date/Time updated: new value is 09/05/2013 08:56

[Start of Response]

Coding and testing of the most major part of this is done. However whilst testing another problem was found by which there is a tiny possibility that an error in the filtering process may not be reported by the Audit Client. This is being investigated.

[End of Response]

Response code to call type L as Category 40 -- Pending -- Incident Under Investigation

Date:13-May-2013 10:48:23 User:Gerald Barnes

Call has been cloned to Call:PC0225656 by User:Gerald Barnes

Date:24-May-2013 10:41:57 User:Gerald Barnes

[Start of Response]

I have now completed initial testing using a debug version and I attach my test plan. Unfortunately 7.22 has been superseded by a 8.01 release and so the fix will need merging with the 8.01 fix. There has been a debate about where exactly this shall be released.

Whilst investigating the original problem the following problems are fixed in QueryDLL.dll

1. The original major problem that transactions would go missing silently from spreadsheets if a evening QueryManager shutdown occurred at a particular point.
2. Due to a bug the QueryManager service does not monitor the spawned QueryHandlers at all on shutdown but simply exits immediately. This meant that the SQL service would shutdown immediately to and the spawned QueryHandlers would have no time to tidy up.
3. Shutting down in the middle of a filter for a FAD code would result in a failure when the QueryManager service came up again.
4. In a FAST ARQ shutting down in the middle of running all queries would result in a failure when the service came up again.
5. In slow ARQs if system errors occurred there was a tiny possibility that they would not be reported.

Once a release is decided on I will do a little more testing (1 week max) of the release (as opposed to debug) build and then do a handover.

[End of Response]

Response code to call type L as Category 40 -- Pending -- Incident Under Investigation
Hours spent since call received: 100 hours

Date: **24-May-2013 12:12:35** User: **Gerald Barnes**
Evidence **Added** - Test Plan

Date: **29-May-2013 11:28:59** User: **John Boston**
Please bear in mind next Audit Maintenance Release is 09.28.

Date: **12-Jun-2013 15:47:59** User: **Gerald Barnes**
The call Target Release has been moved to Proposed For -- HNG-X 09.28

Date: **12-Jun-2013 15:52:23** User: **Gerald Barnes**
[Start of Response]
Andy Dunks has stated that he is prepared to only run audit queries in the day to prevent the possibility of audit transactions being missed from spreadsheets due to a bug in the code that handles the overnight shutdown of the QueryManager service.

I am therefore proposing this PEAK for the 9.28 maintenance release.

[End of Response]
Response code to call type L as Category 55 -- Pending -- Live Fix Impact Supplied
Hours spent since call received: 2 hours

Date: **12-Jun-2013 15:53:03** User: **Gerald Barnes**
Product APOP -- APOP Counter (version unspecified) added.

Date: **12-Jun-2013 15:53:11** User: **Gerald Barnes**
Product APOP -- APOP Counter deleted.

Date: **12-Jun-2013 15:53:25** User: **Gerald Barnes**
Product HNG-X Platforms -- Audit Workstation (AUW) (version unspecified) added.

Date: **12-Jun-2013 15:59:13** User: **Gerald Barnes**
The Business Impact has been updated:
There is a loop hole in the code of QueryDLL.dll where by if it is running during the evening service shutdown the resulting prosecution spreadsheets produced later may have missing transactions.

There is a tiny possibility that errors in the QueryManager service may not be reported meaning that invalid prosecution spreadsheets may be produced.

There is the possibility of errors being generated when audit queries are being run and the QueryManager service is shutdown and restarted. This wastes the time of the prosecution service and makes them rerun queries. This makes achieving SLAs more difficult.

Date: **12-Jun-2013 16:15:43** User: **Gerald Barnes**
Target Date/Time updated: new value is 07/11/2013 08:56
Development Cost updated: new cost is 3 (Man Days)
[Start of Response]
DEVELOPMENT IMPACT OF FIX:

SPECIFY THE HNG-X PLATFORMS IMPACTED:

The platforms have been specified and they are the audit server and audit workstation.

TECHNICAL SUMMARY:

A thorough review of the QueryManager service has been conducted. One major bug has been found which could result in prosecution spreadsheets having missing transactions if the QueryManager service is shutdown and restarted.

In addition many less serious issues have been found with the QueryManager service.

There is a tiny possibility that if an error occurs it will not be reported.

The evening shutdown can cause queries to fail that would otherwise have worked.

These issues are all fixed.

LIST OF KNOWN DIMENSIONS DESIGN PARTS AFFECTED BY THE CHANGE:

AUDIT_EXTRACT_SVR
AUDIT_EXTRACT_CLT

DEPENDENCIES:

There are no particular dependencies.

DEPLOYMENT DETAIL:

The query manager service will need to be stopped and uninstalled.
Files will need to be replaced.
The query manager service will need to be restarted.

DEV EFFORT IN MANDAYS:

3 days further work. Most of the work is already done. However it is checked into VSS in the wrong place because it was originally expected to go at 07.20. This needs sorting out.

IMPACT ON USER:

Prosecution spreadsheets will have less possibility of being incorrect.
Prosecution spreadsheet generation will fail less often.

IMPACT ON OPERATIONS:

Prosecution spreadsheets will have less possibility of being incorrect.
Prosecution spreadsheet generation will fail less often.

HAVE RELEVANT KELS BEEN CREATED OR UPDATED?

The prosecution team is small and they are aware of the issues.

IMPACT ON TEST:

Some prosecution spreadsheets should be generated with no shutdown of the query manager service. Then these same spreadsheets should be produced with multiple shutdown and restarts of the Query Manager service. The end results should always be the same as those produced with no shutdowns.

RISKS (of releasing and of not releasing proposed fix):

If this fix is not delivered there is the possibility that incorrect prosecution spreadsheets will be produced.

If this fix is not delivered some prosecution spreadsheet production runs will fail if the evening shutdown occurs in the middle of them.

LIST OF LIKELY DELIVERABLES:

QueryDll.dll
QueryManager.exe
AECClient.exe

[End of Response]

Response code to call type L as Category 55 -- Pending -- Live Fix Impact Supplied
Hours spent since call received: 1 hours

Date:12-Jun-2013 16:16:40 User:Gerald Barnes
Action placed on Team:RelMngmntForum

Date:17-Jun-2013 14:31:01 User:Lou Barham
The call Target Release has been moved to Targeted At -- HNG-X 09.28

Date:17-Jun-2013 14:31:19 User:Lou Barham
Targeted in PTF as requested

Date:17-Jun-2013 14:31:22 User:Lou Barham
Action has been removed from the call

Date:07-Oct-2013 14:25:02 User:Dimensions Automated User
Reference Added: Product Baseline AUDIT_EXTRACT_CLT_0928_V082
Reference Added: Product Baseline AUDIT_EXTRACT_CLT_0928_V082-V081

Date:07-Oct-2013 16:05:02 User:Dimensions Automated User
Reference Added: Product Baseline AUDIT_EXTRACT_SVR_0928_V067
Reference Added: Product Baseline AUDIT_EXTRACT_SVR_0928_V067-V066

Date:07-Oct-2013 17:28:12 User:Gerald Barnes
I have now finished the regression testing of the server component having merged it in to 9.28. I attach a new test plan which is a rerun of the previous one with a few more tests added. I include the program StartStop.bat which loops around stopping and stopping the Query Manager service which I referred to in the test plan.

Date:07-Oct-2013 17:30:38 User:Gerald Barnes
Evidence Added - Test plan and test program zipped together.

Date:07-Oct-2013 18:23:07 User:Gerald Barnes
[Start of Response]

Fixed by AuditEventMessages.dll, QueryDLL.dll 9.2.8.6, QueryManager.exe 9.2.8.3, RFIDatabase.dll 9.2.8.3, QueryHandler.exe 9.2.8.3 and QueryManager.ini delivered in AUDIT_EXTRACT_SVR_0928_V067-V066.

[End of Response]

Response code to call type L as Category 55 -- Pending -- Live Fix Impact Supplied

Hours spent since call received: 2 hours

Date:07-Oct-2013 18:23:18 User:Gerald Barnes

Defect cause updated to 14: Development - Code

Date:07-Oct-2013 18:23:30 User:Gerald Barnes

The Call record has been transferred to the team: Dev-Int-Rel

Date:08-Oct-2013 11:25:02 User:Dimensions Automated User

Reference Added: Product Baseline AUDIT_EXTRACT_CLT_0928_D082-D081

Date:08-Oct-2013 12:10:01 User:Dimensions Automated User

Reference Added: Product Baseline AUDIT_EXTRACT_SVR_0928_D067-D066

Date:09-Oct-2013 14:17:08 User:PIT Automated User

[Start of Response]

Peak 0225071 handled by integration auto handler

The following baselines attached to this peak have the targeting flags set:

AUDIT_EXTRACT_CLT_0928_D082-D081 FOR (LIVE:YES TEST:YES RDT:YES) Integrator: Geoff Inglis

AUDIT_EXTRACT_SVR_0928_D067-D066 FOR (LIVE:YES TEST:YES RDT:YES) Integrator: Geoff Inglis

These baselines have completed integration testing, moving to holding stack awaiting peak ejection.

[End of Response]

Response code to call type L as Category 47 (Fix Processed by PIT)

The incident has been transferred to the Team: Int-Rel

Date:09-Oct-2013 14:19:17 User:PIT Automated User

[Start of Response]

AUTOMATED UPDATE - INTEGRATION PEAK BOT

Fix processed by integration, routing to dev-int-rel director...

PLEASE NOTE: If this fix has failed, to send this peak back to integration it MUST have the response code Fix Failed or Response Rejected on it, otherwise the peak will bounce.

[End of Response]

Response code to call type L as Category 49 (Fix Available for IndependentTest)

The incident has been transferred to the Team: Live Supp.Test

Date:14-Mar-2014 13:54:56 User:John Rogers

DPVB applied in LST as part of R9.28 Maintenance Release

Following caveat added to release sign-off :-

It was not possible to recreate this issue during pre-installation testing (20 attempts made). During the various phases of post fix testing installation a further 40 attempts were made, again without the problem occurring.

Therefore this area has been successfully regression tested, but it cannot be confirmed that the issue is resolved.

Date:14-Mar-2014 13:55:18 User:John Rogers

Awaiting release to Live

Date:14-Mar-2014 13:55:31 User:John Rogers

The Call record has been transferred to the team: RM-x

Date:19-Nov-2014 14:27:46 User:Lorraine Guiblin

[Start of Response]

Applied to live on HRU10059_PR

[End of Response]

Response code to call type L as Category 60 -- Final -- S/W Fix Available to Call Logger

Routing to Call Logger following Final Progress update.

Date:19-Dec-2014 10:58:01 User:Jason Muir

[Start of Response]

Closing as confirmed complete with Gerald Barnes 19/12/2014

[End of Response]

Response code to call type L as Category 68 -- Final -- Administrative Response
Routing to Call Logger following Final Progress update.

Date:19-Dec-2014 10:58:07 User:Jason Muir
CALL PC0225071 closed: Category 68 Type L

Root Cause	Development - Code
Logger	Andy Dunks -- Security Ops
Subject Product	General/Other/Misc -- Unknown General/Other/Misc (version unspecified)
Assignee	Andy Dunks -- Security Ops
Last Progress	19-Dec-2014 10:58 -- Jason Muir