FUJ00171848

Export

Peak Incident Management System

Call Reference	**PC0205805**	Call Logger	Deleted User -- Security Ops
Release	Targeted At -- HNG-X 03.24	Top Ref	AUDIT_EXTRACT_SVR_0324_D056-D055
Call Type	Vulnerability	Priority	B -- Important
Contact	Deleted Contact	Call Status	Closed -- S/W Fix Available to Call Logger
Target Date	24/12/2010	Effort (Man Days)	2.00
Summary	Audit - Duplicate Message sequences are not recorded by Fast ARQ retrieval		

All References	Type	Value
	Call reference	PC0206590
	Product Baseline	AUDIT_EXTRACT_SVR_0324_V056
	Call reference	PC0206622
	Product Baseline	AUDIT_EXTRACT_SVR_0324_V056-V055
	Call reference	PC0206697
	Product Baseline	AUDIT_EXTRACT_SVR_0324_D056-D055
	Call reference	PC0206827
	DevIntRel-Director	Live Supp.Test
	Release PEAK	PC0207465

Impact Statement	User	Date
	Gerald Barnes	05-Nov-2010 11:49:40
	The Fast ARQ interface does not provide the user with any indication of duplicate records/messages. This omission means that we are unaware of the presence of duplicate transactions. In the event that duplicates are retrieved and returned to POL without our knowledge the integrity of the data provided comes into question. The customer and indeed the defense and the court would assume that the duplicates were bone fide transactions and this would be incorrect. There are a number of high profile court cases in the pipeline and it is imperative that we provide sound, accurate records.	

Progress Narrative

Date:**27-Oct-2010 11:41:05** User:**Penny Thomas**
CALL PC0205805 opened
Details entered are:-
Summary:Audit - Duplicate Message sequences are not recorded by Fast ARQ retrieval
Call Type:V
Call Priority:B
Target Release:HNG-X R2
Routed to:Security Ops - Penny Thomas

Date:**27-Oct-2010 11:48:13** User:**Penny Thomas**
The Fast ARQ interface does not provide the user with any indication of duplicate records/messages.

This omission means that we are unaware of the presence of duplicate transactions. In the event that duplicates are retrieved and returned to POL without our knowledge the integrity of the data provided comes into question. The customer and indeed the defense and the court would assume that the duplicates were bone fide transactions and this would be incorrect. There are a number of high profile court cases in the pipeline and it is imperative that we provide sound, accurate records.

Date:**27-Oct-2010 11:48:44** User:**Penny Thomas**
The Call record has been transferred to the team: Audit-Dev
The Call record has been assigned to the Team Member: Andrew Mansfield

Date:**29-Oct-2010 14:02:55** User:**Andrew Mansfield**
The Call record has been assigned to the Team Member: Gerald Barnes

Date:**01-Nov-2010 10:51:37** User:**Gerald Barnes**
Target Date/Time updated: new value is 02/11/2010 11:41
[Start of Response]
Andy and I have looked at this. We think the method most compatible with existing behaviour is as follows -

FUJ00171848

Check for duplicates for HNGx in a similar method to how duplicates are checked for in Horizon. For Horizon they are legitimately logged in the audit log and then ignored (because it is just that identical messages are stored by mistake in more than one transaction file). For HNGx, in the Fast ARQ case, their detection will cause them to be logged in the QueryLog and a count kept of how many there are; they will not be ignored.

If this count is greater than 0 then bError will be set and the block of code

```
      if (bError)
      {
         //The Fast ARC must be stopped.
         CTraceFile::Trace(TL_ERROR,"The Fast ARQ is being terminated because there are %ld crypto errors, %ld errors and %ld
gaps found.",lTotalCryptoErrors,lTotalErrorsFound,lTotalGapsFound);
         setStatus(CRFIQueryRequest::E_ABSTRACT_FILES_FAILED);
         return;
      }
```

modifed to log the number of duplicates found.

I will produce a prototype to confirm that behaviour is acceptable.
[End of Response]
Response code to call type V as Category 40 -- Pending -- Incident Under Investigation
Hours spent since call received: 2 hours

Date:**05-Nov-2010 11:16:40** User:**Gerald Barnes**
[Start of Response]
I have built a prototype QueryDLL.dll which solves this problem. Now if duplicate HNGx messages are detected the Fast ARQ fails at the client with the message "Filtering Failed" displayed at the bottom of its form and on the server in the QueryLog there are detailed messages describing the duplicates found.

I attach a zip of the source (with the changes done marked up by this PEAK number) plus details of the test run in a test plan in evidence attached and labelled "Prototype Fix".
[End of Response]
Response code to call type V as Category 38 -- Pending -- Potential Problem Identified
Hours spent since call received: 15 hours

Date:**05-Nov-2010 11:22:30** User:**Gerald Barnes**
Evidence **Added** - Prototype Fix

Date:**05-Nov-2010 11:47:56** User:**Gerald Barnes**
[Start of Response]
DEVELOPMENT IMPACT OF FIX:

SPECIFY THE HNG-X PLATFORMS IMPACTED:

The platform is set and is the "Audit Server".

TECHNICAL SUMMARY:

HNGx can rarely produce transactions with duplicate Journal Sequence Numbers. At the moment, when running a FAS ARQ on the audit server, these duplicates are not noticed. This means that the evidence presented by the Prosecution Team may show duplicate transactions without it being noticed; the Defence Team may spot this and call into the question the integrity of our data.

LIST OF KNOWN DIMENSIONS DESIGN PARTS AFFECTED BY THE CHANGE:

AUDIT_EXTRACT_SVR

ARE ANY OF THESE DESIGN PARTS AFFECTED BY APPROVED CPs/PEAKS in HNGX Release 2:

Yes they are, but HNGX Release 2 has been live for quite a while.

RELEASE 2 IMPACT:

The change affects FAST ARQs; FAST ARQs were brought in at Release 2.

DEPENDENCIES:

This fix has no particular dependencies.

DOES THE FIX REQUIRE ANY MANUAL DEPLOYMENT BASELINES:

The fix does not require any manual installation; it will just be a replacement file.

DEV EFFORT IN MANDAYS:

The coding of the fix is complete, however further regression tests need to be run.

2 days for further regression tests and the handover.

IMPACT ON USER:

HNGx transactions with duplicate JSNs may not be noticed. This will call into question the reliability of evidence presented by the prosecution team.

IMPACT ON OPERATIONS:

The prosecution evidence will be more consistent and so prosecution cases will go though more smoothly.

FUJ00171848

HAVE RELEVANT KELS BEEN CREATED OR UPDATED?

It was not felt that a KEL was required because there are only two people in the prosecution team and they are both fully aware of the problem.

IMPACT ON HORIZON TO HNGX BRANCH MIGRATIONs

There is no impact on migration to HNGx. All offices are now migrated to HNGx and so it is impossible that anything would affect this now.

IMPACT ON TEST:

The test team need to regression test Fast ARQs and filtering in slow ARQs. They need to run some specific tests when there are duplicate Horizon transactions (they should just be ignored as they are at the moment) and duplicate HNGx transactions (they will now cause a Fast ARQ to fail which used not to be the case).

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

If the fix is not released then duplicate HNGx transactions will continue not to be noticed by the prosecution team which will call into question their evidence.

There are no particular risks in releasing the fix. All QueryDLL fixes supplied recently have gone though with no reported problems.

LIST OF LIKELY DELIVERABLES:

QueryDLL.dll

LIST OF THE ABOVE ALREADY DELIVERED FOR THE PROPOSED RELEASE:

None.

LIST OF THE ABOVE ALREADY DELIVERED TO A RELEASE LATER THAN THAT PROPOSED:

None.

LIST OF THE ABOVE LIKELY TO BE REDELIVERED INTO THE PROPOSED OR A LATER RELEASE:

QueryDLL.dll
[End of Response]
Response code to call type V as Category 55 -- Pending -- Live Fix Impact Supplied
Hours spent since call received: 1 hours

Date:**05-Nov-2010 11:48:31** User:**Gerald Barnes**
Product HNG-X Platforms -- Audit Server (ARC) (version unspecified) added.

Date:**05-Nov-2010 11:48:36** User:**Gerald Barnes**
Product HNG-X Platforms -- Audit Workstation (AUW) deleted.
Product HNG-X Platforms -- Audit Server (ARC) updated to Subject.

Date:**05-Nov-2010 11:49:40** User:**Gerald Barnes**
A new Business Impact has been added:
The Fast ARQ interface does not provide the user with any indication of duplicate records/messages.

This omission means that we are unaware of the presence of duplicate transactions. In the event that duplicates are retrieved and returned to POL without our knowledge the integrity of the data provided comes into question. The customer and indeed the defense and the court would assume that the duplicates were bone fide transactions and this would be incorrect. There are a number of high profile court cases in the pipeline and it is imperative that we provide sound, accurate records.

Date:**05-Nov-2010 11:50:36** User:**Gerald Barnes**
The call Target Release has been moved to Requested For -- HNG-X 04.37

Date:**05-Nov-2010 11:52:23** User:**Gerald Barnes**
Target Date/Time updated: new value is 01/03/2011 11:41
Development Cost updated: new cost is 2 (Man Days)
[Start of Response]
I update the Development (ManDays) field.
[End of Response]
Response code to call type V as Category 55 -- Pending -- Live Fix Impact Supplied

---

Date:**05-Nov-2010 11:53:24** User:**Gerald Barnes**
Action placed on Team:Audit-Dev, User:Gerald Barnes

Date:**05-Nov-2010 11:54:10** User:**Gerald Barnes**
Action has been removed from the call

Date:**05-Nov-2010 11:54:32** User:**Gerald Barnes**
Action placed on Team:RelMngmntForum

FUJ00171848

Date:**05-Nov-2010 16:13:09** User:**Gerald Barnes**
Product HNG-X Platforms -- Audit Server (ARC) (version unspecified) added.

Date:**08-Nov-2010 11:28:53** User:**Tyrone Cozens**
The call Target Release has been moved to Targeted At -- HNG-X 04.37

Date:**08-Nov-2010 11:28:56** User:**Tyrone Cozens**
Action has been removed from the call

Date:**08-Nov-2010 11:29:07** User:**Tyrone Cozens**
Authorised for 04.37 as agreed with RMF members.

Date:**08-Nov-2010 12:34:48** User:**Gerald Barnes**
Target Date/Time updated: new value is 30/03/2011 11:41
[Start of Response]
A fix has been prepared. It just needs merging into the source in VSS, some additional regression testing and handing over.
[End of Response]
Response code to call type V as Category 46 -- Pending -- Product Error Fixed
Hours spent since call received: 1 hours

Date:**24-Nov-2010 16:45:20** User:**Andrew Mansfield**
Sarah Selwyn has requested an audit maintenance release prior to the next DC_AUDIT planned release due to go live on 14/05/2011.

Five Peaks are requested for this maintenance release: PC0205805, PC0205806, PC0206531, PC0206590, PC0206622.

This is an edited version of the text of Sarah's original email to Sheila Bamber:

We would like to get these Peaks targeted ASAP since these are impacting SSC and the Litigation Support Group in their support of the Post Office litigations. There is a risk that these teams will not be able to fulfil their OLTs to the Post Office as defined in SVM/SDM/SD/0017 (Security Service Management: Service Description).

We would like to request an earlier test and deployment slot for PEAKs that are causing a significant business impact on the SSC and Litigation Support teams ? the PEAKs for earlier deployment are:

PC0205805 and PC025806 - Litigation Support Group need to detect/highlight duplicate JSNs - enhancements to AUW to support duplicate JSN detection and reporting
PC0206531 - SSC ? takes too long to analyse events associated with ARQs due to the large volume of BAL events requires a change to the filtering of financially significant vs benign events. A change to the presentation of the events to SSC is also required to speed the process up.

Testing requirements:

PC0205805 and PC025806 ? use test files which include duplicate HNG-X transactions perform Fast ARQs which will now not fail on duplicate detection and checking the spreadsheet output which will now report overlaps and duplicates. Test Horizon ARQs with duplicate JSN present to show duplicates ignored. Regression test for files with no duplicate JSNs both fast ARQ and filtering in slow ARQs.
The BAL events reported in the event files output will now be of a smaller volume, nominated benign events will appear in the rejects files (and this will constitute a large volume of total events) and the events spreadsheet will have a column heading at the top of the spreadsheet. Regression test Gaps reporting is still present on spreadsheets. If time permits the workbook with a number of spreadsheets as described in the PEAK rather than by manual process by the litigation team. However, this is yet to be confirmed.

(Since Sarah's original email PC0206590 and PC0206622 have been raised to deal with issues around the large number of events. PC0206531 is now solely to deal with the presentation of events.)

Date:**24-Nov-2010 16:49:18** User:**Andrew Mansfield**
Action placed on Team:RelMngmntForum

Date:**25-Nov-2010 16:11:07** User:**Tyrone Cozens**
On hold until new ''Audit'' release decided (Adam Spurgeon looking into).

Date:**03-Dec-2010 10:38:01** User:**Tyrone Cozens**
The call Target Release has been moved to:Targeted At -- HNG-X 03.24
Authorised for 03.24 as agreed with Mark Jepson.

Date:**03-Dec-2010 10:38:10** User:**Tyrone Cozens**
Action has been removed from the call

FUJ00171848

Date:**03-Dec-2010 11:41:12** User:**Gerald Barnes**
Target Date/Time updated: new value is 24/12/2010 11:41
[Start of Response]
A fix will now be prepared and tested. It will then be stored in VSS-InfDom. It will be handed over on the 24th December.
[End of Response]
Response code to call type V as Category 40 -- Pending -- Incident Under Investigation

Date:**14-Dec-2010 17:18:50** User:**Gerald Barnes**
[Start of Response]
It has now been decided that the detection of duplicate HNGx messages will not terminate the FAST ARCs. Duplicates will be logged by QueryDLL at the server initially in QueryHandler.log and eventually in the close log both for Horizon and HNGx transactions. Duplicate HNGx transactions will also be logged by the client in its spreadsheets but duplicate Horizon transactions will be eliminated at the server silently since they are known always to be benign.
[End of Response]
Response code to call type V as Category 46 -- Pending -- Product Error Fixed
Hours spent since call received: 4 hours

Date:**22-Dec-2010 10:48:52** User:**Gerald Barnes**
Reference Added: Call reference PC0206590

Date:**22-Dec-2010 10:49:17** User:**Gerald Barnes**
Reference Added: Call reference PC0206622

Date:**22-Dec-2010 10:49:37** User:**Gerald Barnes**
Reference Added: Call reference PC0206697

Date:**22-Dec-2010 10:50:06** User:**Gerald Barnes**
Reference Added: Call reference PC0206827

Date:**22-Dec-2010 10:51:49** User:**Gerald Barnes**
[Start of Response]
I add a test report for this PEAK and the four associated PEAKs PC0206590, PC0206622, PC0206697 and PC0206827.
[End of Response]
Response code to call type V as Category 46 -- Pending -- Product Error Fixed
Hours spent since call received: 37 hours

Date:**22-Dec-2010 10:52:44** User:**Gerald Barnes**
Evidence **Added** - Test Report

Date:**29-Dec-2010 12:35:04** User:**PIT Automated User**
Reference Added: Product Baseline AUDIT_EXTRACT_SVR_0324_V056
Reference Added: Product Baseline AUDIT_EXTRACT_SVR_0324_V056-V055

Date:**29-Dec-2010 12:41:58** User:**Gerald Barnes**
[Start of Response]
Fixed by version 4.1.0.1 of NWB_Legato_Recover.exe and version 4.0.0.4 of QueryDLL.dll handeed over in AUDIT_EXTRACT_SVR_0324_V056-V055.
[End of Response]
Response code to call type V as Category 46 -- Pending -- Product Error Fixed
Hours spent since call received: 4 hours

Date:**29-Dec-2010 12:42:13** User:**Gerald Barnes**
The Call record has been transferred to the team: Dev-Int-Rel

Date:**31-Dec-2010 08:05:04** User:**PIT Automated User**
Reference Added: Product Baseline AUDIT_EXTRACT_SVR_0324_D056-D055

Date:**05-Jan-2011 08:28:27** User:**Lionel Higman**
[Start of Response]
.
[End of Response]
Response code to call type V as Category 49
The Call record has been transferred to the team: Live Support Team
The Call record has been assigned to the Team Member: _Unassigned_

Date:**11-Jan-2011 09:46:55** User:**Victoria Hancock**
Reference Added: Release PEAK PC0207465

Date:**19-Jan-2011 14:16:04** User:**John Rogers**
[Start of Response]
Tested in LST as part of Audit Release 3.24

Duplicate message sequences are now recorded in the Query Handler and Closure (RFI) log files, for both Slow and Fast ARQs.

FUJ00171848

[End of Response]
Response code to call type V as Category 60 -- Final -- S/W Fix Available to Call Logger
Routing to Call Logger following Final Progress update.
Defect cause updated to 7 -- Design - High Level Design

Date:**19-Jan-2011 15:03:29** User:**John Rogers**
The Call record has been transferred to the team: Live Supp.Test
The Call record has been assigned to the Team Member: Release to Live

Date:**16-Mar-2011 15:20:06** User:**Mark Ascott**
The Call record has been transferred to the team: RM-x

Date:**27-Apr-2011 16:02:21** User:**John Budworth**
[Start of Response]
Applied to live 03/02/2011 as part of Audit Release 03.24.
[End of Response]
Response code to call type V as Category 60 -- Final -- S/W Fix Available to Call Logger
Routing to Call Logger following Final Progress update.

Date:**27-Apr-2011 16:04:51** User:**Penny Thomas**
CALL PC0205805 closed: Category 60 Type V

Root Cause	Design - High Level Design
Logger	Deleted User -- Security Ops
Subject Product	HNG-X Platforms -- Audit Server (ARC) (version unspecified)
Assignee	Deleted User -- Security Ops
Last Progress	27-Apr-2011 16:04 -- Penny Thomas