BEATRICE CARDONA

BARBARA VANDEN BORRE

WEN TANG

January 22, 2010

Re: Release: 1903
Error Reports: 2244
Programs: PPWEBSEC
Copy Members: None
Include Members: None
DDL Members: None
Bind Members: None
CICS Maps: None
CICS Help: None
Forms: None
Table Updates: None
Urgency: Not Urgent (see Timing of Installation below)

This release addresses the following Error Report(s):

Error Report 2244

CICS transaction security for Web Services is established by release 1862. While the configuration created by R1862 will work, a different one has been developed in consultation with the mainframe systems and hosted applications group at UCOP. The new configuration is easier to work with and provides an easier way to audit which web application servers have access to any given CICS region.

Programs

PPWEBSEC

PPWEBSEC will switch to transaction UCIH (this is a new transaction code that is not currently in BASE) at the same time it switches to the logged on end user id. UCIH should be available to the same RACF groups that currently are allowed to use the PPS EDB Entry update main transaction.

Installation Instructions

Install, compile, and link the following modified program:

<table>
<thead>
<tr>
<th>PROGRAM</th>
<th>DB2?</th>
<th>Compile Type</th>
<th>Package Bind?</th>
<th>Done?</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPWEBSEC</td>
<td>NO</td>
<td>CICS</td>
<td>NO</td>
<td></td>
</tr>
</tbody>
</table>
Install new CICS transaction UCIH

Edit CARDLIB member RDOPROD by replacing *GROUPID* with the appropriate local RDO group name and *PLAN* with the appropriate plan name. Apply the updates to the appropriate CSD file.

Implement transaction security

These changes are intended to ensure that:

- Web Services hosted by a CICS region (which are always run under transaction CPIH to start) can only be used by a RACF group that contains only RACF ids associated with client certificates owned by web servers that are authorized to use Web Services in that region.

- PPS application logic run as part of the Web Service (which will always run under transaction UCIH) can only be used by authorized users and groups.

Complete the following steps for all CICS regions that will host PPS Web Services:

- If it does not already exist, create RACF profile CICSXXXX.CPIH in class TCICSTRN (where CICS region’s userid is CICSXXXX)

- Revoke any existing READ access to CICSXXXX.CPIH

- Create RACF group GWEBXXXX; add the RACF id associate with each client certificate that will be allowed to use CPIH in region CICSXXXX to group GWEBXXXX

- Permit READ access to CICSXXXX.CPIH to RACF group GWEBXXXX.

- Do not permit READ access to CICSXXXX.CPIH to the default userid of region CICSXXXX

- Create RACF profile CICSXXXX.UCIH in class TCICSTRN (where CICS region userid is CICSXXXX)

- Permit READ access to CICSXXXX.UCIH to all users and groups allowed to access PPS in the CICS region.

- Do not permit READ access to CICSXXXX.UCIH to the default userid of region CICSXXXX
Test Plan

In CICS region CICSXXXX

- [action]
  - [expected response]
- Key in CLEAR
  - Cleared screen
- Key in CPIH and press ENTER.
  - DFHAC2002 MM/DD/YYYY HH:MM:SS A10CDPP2 To use this transaction CPIH you must sign on or have the right security level.
- Key in UCIH and press ENTER
  - DFHAC2016 MM/DD/YYYY HH:MM:SS A10CDPP2 Transaction UCIH cannot run because program ZZZZZZZZ is not available.
- Key in CEDX UCIH
  - TRANSACTION UCIH: EDF ON
- Log into the PPS web main menu instance which uses Web Services in CICSXXXX
  - In CICSXXXX, CEDF debug screen displays and contains text “EIBTRNID = ‘UCIH’”
- Key F3
  - EDF SESSION TERMINATED

Timing of Installation

The timing of this release is not urgent.

As usual, campuses are encouraged to install this release in as timely a fashion as possible and in the normal numeric sequence.

If there are any questions, please send electronic mail to Peter.Parker@ucop.edu or call 510 987-0908.

Peter Parker