VistA Patch Display Page: 1

=============================================================================

Run Date: MAR 08, 2016 Designation: XU\*8\*659 TEST v9

Package : KERNEL Priority : MANDATORY

Version : 8 Status : UNDER DEVELOPMENT

=============================================================================

Associated patches: (v)XU\*8\*430 <<= must be installed BEFORE `XU\*8\*659'

(v)XU\*8\*504 <<= must be installed BEFORE `XU\*8\*659'

(v)XU\*8\*584 <<= must be installed BEFORE `XU\*8\*659'

(v)XU\*8\*638 <<= must be installed BEFORE `XU\*8\*659'

(v)XU\*8\*655 <<= must be installed BEFORE `XU\*8\*659'

Subject: SINGLE SIGN-ON PROVISIONING AND IMPLEMENTATION

Category: ENHANCEMENT

ROUTINE

PRINT TEMPLATE

OTHER

DATA DICTIONARY

Description:

===========

This patch provides enhancements needed to implement Single Sign-On

Internal (SSOi) for identification and authentication of users into VistA.

VAIQ #7613595 "Mandatory Use of PIV Multifactor Authentication to VA

Information Systems" dated June 30, 2015, requires all VA IT systems to be

PIV-enabled and requires the use of multifactor authentication when using

a local, network, or remote account to log into a VA information system.

This patch provides the VistA Kernel utilities needed to implement this

requirement.

The use of these utilities are expected to improve security and auditing

capabilities in accordance with VA Handbook 6500 Appendix F and revision 4

of NIST SP 800-53. As required by FIPS 199 and using guidance from NIST SP

800-60, the recommended security categorization for these applications is

HIGH.

Integration with Identity and Access Management (IAM) services are

mandated by executive management via the following memorandums:

- IAM Identity Services (IdS) mandate memorandum (VAIQ #7011145). All

applications within VA must comply with IAM requirements to ensure that

references to the identities of Veterans and their beneficiaries are

accurate.

- IAM Access Services (AcS) functionality within VA is mandated by VAIQ

#7060071 (xxxxxxx).

The following changes have been made to implement SSOi in VistA:

Identity and Access Management (IAM)

- This patch adds or updates Remote Procedures to provide Kernel support

for the IAM Provisioning and IAM Binding applications.

- This patch adds or updates Remote Procedures to fully implement Kernel

processing of IAM Secure Token Service (STS) tokens for secure

authentication and identification of users authenticated by IAM using

Active Directory credentials (KERBEROS or PIV Card).

- The XUS IAM BIND USER and XUS ESSO VALIDATE Remote Procedures have

been added to the XUS SIGNON menu option to make them available to all

users.

VistA Kernel Security

- Per the VA Authentication, Authorization, and Audit (AAA) Design

Pattern, VA Applications shall implement Level of Assurance (LOA)

requirements for authentication. VA shall use guidance from OMB 04-04

and NIST SP 800-63-2 to rate all existing applications to their

appropriate LOA and implement appropriate security controls for user

authentication to those applications. LOA for a user's authentication

shall be determined by the weakest link in the authentication process.

Application authentication protocols shall comply with all existing

policy established in VA 6500.

- This patch identifies the sign-on LOA when authenticating a user into

VistA using traditional and newly-developed authentication methods.

- This patch records the LOA in the SIGN-ON LOG file (#3.081) if the

information is available.

- In the future, when LOA identification is fully implemented into Kernel

Security, access to VistA will be denied when little or no confidence

exists in the asserted user identity (DUZ("LOA")=1). Until then, VistA

application developers can choose to limit or deny access to individual

applications or data when DUZ("LOA")=1.

Veterans Access, Choice, and Accountability Act of 2014 (VACAA)

- This patch updates the API introduced in XU\*8.0\*655 to bulk-load non-VA

entities and providers. The updated API provides a means of making

recurring updates to the NEW PERSON file (#200) to identify non-VA

providers when documenting patient care. The API is provided to

Outpatient Pharmacy under private Integration Agreement #6230.

Blood Bank Clearance

====================

Clearance - 01/13/2015

EFFECT ON BLOOD BANK FUNCTIONAL REQUIREMENTS: Patch XU\*8.0\*659 contains

changes to a package referenced in ProPath standard titled BBM Team

Review of VistA Patches. This patch does not alter or modify any VistA

Blood Bank software design safeguards or safety critical elements

functions.

RISK ANALYSIS: Changes made by patch XU\*8.0\*659 have no effect on Blood

Bank software functionality, therefore RISK is none.

Patch Components

================

Files & Fields Associated:

File Name (Number) Field Name (Number) New/Modified/Deleted

------------------ ------------------- --------------------

KERNEL SYSTEM PARAMETERS (#8989.3)

SECURITY TOKEN SERVICE (#200.1) New

ORGANIZATION (#200.2) New

ORGANIZATION ID (#200.3) New

SIGN-ON LOG (#3.081) LEVEL OF ASSURANCE (#101) New

Forms Associated:

Form Name Type New/Modified/Deleted

--------- ---- --------------------

N/A

Options Associated:

Option Name Type New/Modified/Deleted

----------- ---- --------------------

XUS SIGNON Broker (Client/Server) MODIFIED

XUS VISIT USERS Print MODIFIED

XUSEC REMOTE ACCESS Print MODIFIED

Protocols Associated:

--------------------

N/A

Security Keys Associated:

------------------------

N/A

Templates Associated:

Template Name Type File Name (Number) New/Modified/Deleted

------------- ---- ------------------ --------------------

XUSEC LIST Print SIGN-ON LOG (3.081) Modified

XUSEC REMOTE ACCESS Print SIGN-ON LOG (3.081) Modified

Remote Procedure Calls Associated:

RPC Name Type New/Modified/Deleted

-------- ---- --------------------

XUS ALLKEYS PUBLIC Modified (description only)

XUS AV CODE RESTRICTED Modified (description only)

XUS BSE TOKEN SUBSCRIPTION New

XUS CVC RESTRICTED Modified (description only)

XUS ESSO VALIDATE RESTRICTED Modified

XUS IAM ADD USER SUBSCRIPTION Modified

XUS IAM BIND USER SUBSCRIPTION Modified

XUS IAM DISPLAY USER SUBSCRIPTION Modified

XUS IAM EDIT USER SUBSCRIPTION Modified

XUS IAM FIND USER SUBSCRIPTION Modified

XUS IAM REACTIVATE USER SUBSCRIPTION New

XUS IAM TERMINATE USER SUBSCRIPTION New

XUS KAAJEE GET CCOW TOKEN RESTRICTED Modified (description only)

XUS KAAJEE GET USER INFO AGREEMENT Modified (description only)

XUS KAAJEE GET USER VIA PROXY RESTRICTED Modified (description only)

XUS KAAJEE GET LOGOUT AGREEMENT Modified (description only)

XUS KEY CHECK PUBLIC Modified (description only)

XUS SIGNON SETUP SUBSCRIPTION Modified (description only)

New Service Requests (NSRs)

----------------------------

N/A

Patient Safety Issues (PSIs)

-----------------------------

N/A

Remedy Ticket(s) & Overview

---------------------------

I5606567FY15 VAIQ #7060071 IAM Access Services (AcS) functionality

1. I5606567FY15 VAIQ #7060071 IAM Access Services (AcS) functionality

Problem:

-------

Integration with Identity and Access Management (IAM) services are

mandated by executive management via VAIQ #7011145 and VAIQ #7060071.

Resolution:

----------

This patch provides the finished interfaces to identify and authenticate

a user into VistA using a Security Assertion Markup Language (SAML) token

from the IAM Secure Token Service (STS), and provides the interfaces for

an IAM Provisioning application to configure users to be identified by

SAML token.

Test Sites: (Patch Tracking Message #76891612)

----------

[Potential test sites - Update list and remove POCs before release]

Boise VA Medical Center, Boise ID (xxx - Medium)

[xxx and xxxx]

Cheyenne VA Medical, Cheyenne WY (xx - Medium)

[xxx and xxxxx]

xxxx Veterans Affairs Medical Center, Milwaukee WI (xxx -

Large)

[xxxxx]

Hampton VA Medical Center, Hampton VA (xxx - Large)

[xxxx]

Hunter Holmes McGuire VA Medical Center, Richmond VA (652 - Large)

[xxxxx]

Memphis VA Medical Center, Memphis TN (xx - Large)

[xxxxx]

Minneapolis VA Medical Center, Minneapolis MN (xx - Large)

[xxxx]

Philadelphia VA Medical Center, Philadelphia PA (xxx - Large)

VA Central Western Massachusetts HCS (Northampton), Leeds MA (xxx -

Medium)

[xxxx]

VA Gulf Coast Veterans Health Care System, Biloxi MS (xxx – Large)

[Kathy Taylor]

VA Hudson Valley HCS, Montrose NY (xxx - Integrated)

VA Puget Sound Health Care System, Seattle WA (xxx - Integrated)

[xxx and xxx]

VA South Texas Veterans Health Care System, San Antonio TX (xxx -

Integrated)

[xxxxx]

Washington DC VA Medical Center, Washington DC (xxx - Large)

Documentation Retrieval Instructions

------------------------------------

No changes have been made to Kernel documentation as a result of this

patch. However, the most up-to-date VA Kernel end-user documentation

is available on the VHA Software Document Library (VDL) at the following

Internet Website:

NOTE: VistA documentation is made available online in Microsoft Word

format (.DOC) and Adobe Acrobat Portable Document Format (.PDF).

Patch Installation:

Pre-Installation Instructions

-----------------------------

This patch can be NOT be queued for installation, since the post-

installation routine requires interactive input. TaskMan does not have to

be stopped, HL7 filers do not need to be stopped, and users may be on the

system. There are no menu options or protocols that need to be disabled.

Installation Instructions

-------------------------

This patch may be installed with users on the system. This patch should

take less than 1 minute to install. It may be queued for installation.

There are no options that need to be disabled.

1. Choose the PackMan message containing this patch.

2. Choose the INSTALL/CHECK MESSAGE PackMan option.

3. From the Kernel Installation and Distribution System Menu, select

the Installation Menu. From this menu, you may elect to use the

following option. When prompted for the INSTALL enter the patch #(ex.

XU\*8.0\*659):

a. Print Transport Global - This option lets you print the contents

of a Transport Global that is currently loaded in the ^XTMP

global.

b. Backup a Transport Global - This option will create a backup

message of any routines exported with this patch. It will not

backup any other changes such as DDs or templates.

c. Compare Transport Global to Current System - This option will

allow you to view all changes that will be made when this patch

is installed. It compares all components of this patch

(routines, DDs, templates, etc.).

d. Verify Checksums in Transport Global - This option will allow

you to ensure the integrity of the routines that are in the

transport global.

4. From the Installation Menu, select the Install Package(s) option and

choose the patch to install.

5. If prompted 'Want KIDS to Rebuild Menu Trees Upon Completion of

Install? NO//' answer "NO".

6. When prompted 'Want KIDS to INHIBIT LOGONs during the install?

NO//' answer "NO".

7. If prompted 'Want to DISABLE Scheduled Options, Menu Options,

and Protocols? NO//' answer "NO".

8. If prompted 'Delay Install (Minutes): (0 - 60): 0//' answer "0" to

"60" or "Q" (to queue the output to a printer).

Post-Installation Instructions

------------------------------

There are no post-installation tasks. A post-installation routine will

run upon patch installation to install data in specific locations. The

expected output will be similar to the following. If your output shows

error messages, an incident ticket should be opened to troubleshoot your

patch installation.

OPTION exists at IEN = 11418

REMOTE APPLICATION entry created: IAM PROVISIONING

OPTION exists at IEN = 11419

REMOTE APPLICATION entry created: IAM BINDING

OPTION WEBN NATL UTIL MGMT INTEG created

REMOTE APPLICATION entry created: NUMI

OPTION WEBB BED MGMT SOLUTION created

REMOTE APPLICATION entry created: BMS

DIALOG entry created: STS token not valid.

KERNEL SYSTEM PARAMETERS fields populated: SECURITY TOKEN SERVICE,

ORGANIZATION, ORGANIZATION ID

Routine Information:

====================

The second line of each of these routines now looks like:

;;8.0;KERNEL;\*\*[Patch List]\*\*;Jul 10, 1995;Build 22

The checksums below are new checksums, and

can be checked with CHECK1^XTSUMBLD.

Routine Name: XLFNSLK

Before: B44384655 After: B39616756 \*\*142,151,425,638,659\*\*

Routine Name: XU8PS655

Before:B102640640 After: Delete

Routine Name: XU8PS659

Before: n/a After: B63050406 \*\*659\*\*

Routine Name: XUCERT

Before: n/a After: B4132125 \*\*659\*\*

Routine Name: XUCERT1

Before: n/a After: B20606802 \*\*659\*\*

Routine Name: XUESSO1

Before: B77693554 After: B93859687 \*\*165,183,196,245,254,269,337,

395,466,523,655,659\*\*

Routine Name: XUESSO2

Before:B108993229 After:B117714262 \*\*655,659\*\*

Routine Name: XUESSO3

Before:B206943521 After:B221983051 \*\*655,659\*\*

Routine Name: XUESSO4

Before: n/a After: B61505269 \*\*659\*\*

Routine Name: XUP

Before: B11551061 After: B11898665 \*\*208,258,284,432,469,659\*\*

Routine Name: XUS

Before: B31567708 After: B35560117 \*\*16,26,49,59,149,180,265,337,

419,434,584,659\*\*

Routine Name: XUS1

Before: B28568204 After: B29132312 \*\*9,59,111,165,150,252,265,419,

469,523,543,638,659\*\*

Routine Name: XUSAML

Before: B78896546 After: B87822485 \*\*655,659\*\*

Routine Name: XUSBSE1

Before:B117144392 After:B158984065 \*\*404,439,523,595,522,638,659\*\*

Routine Name: XUSHSH

Before: B31040658 After: B37891600 \*\*655,659\*\*

Routine Name: XUSKAAJ

Before: B11629985 After: B11718164 \*\*329,430,659\*\*

Routine Name: XUSKAAJ1

Before: B1687417 After: B2125056 \*\*504,659\*\*

Routine Name: XUSRB

Before: B33401626 After: B35393386 \*\*11,16,28,32,59,70,82,109,115,

165,150,180,213,234,238,265,

337,395,404,437,523,659\*\*

Routine Name: XUSRB4

Before: B18435992 After: B20805610 \*\*150,337,395,419,437,499,523,

573,596,638,659\*\*

Routine list of preceding patches: 430, 504, 584, 638, 655

=============================================================================

User Information:

Entered By : xxxxx Date Entered : MAY 21,2015

Completed By: Date Completed:

Released By : Date Released :

=============================================================================