

Title: Assuria Auditor AutoUpdate #105 released
Number: 10 / 06 **Date: 28 February 2010**

Title Assuria Auditor AutoUpdate #105 released

Introduction

This update is an Assuria content update. The update is compatible with, and suitable for application to all Assuria Auditor agents.

Contents

Conformance checking for GCSX Code of Connection

Additional checks have been added to all supported operating systems, in order to support conformance checking for the UK Government Secure Extranet Code of Connection version 4.1, for English and Welsh Local Authorities commonly known as GCSX CoCo.

These include checks for:

- Servers running DHCP
- Time servers daemons/services and settings
- Domain GPO settings for access to removable media (Microsoft Windows Server 2008 and Vista)

The new checks are applicable to all users and included in the appropriate policies.

The UK Government Secure Extranet Code of Connection has been added to the set of standards supported by Assuria Auditor. This includes a mapping of existing and new checks to that standard, inclusion of standards information in the policy navigators, and the ability to report on vulnerabilities grouped by the appropriate section of the GCSX CoCo standard.

Windows Server 2008

In developing Remote Adapter support for Windows Server 2008 R2 and over 65 new checks were developed and these are made available in this AutoUpdate for Windows Server 2008.

Additional checks for Microsoft Windows server 2008 GPO security settings

A number of new checks have been written to check Group Policy Security Options settings.

Enhancement to Inventory Baseline

The Inventory Baseline has been enhanced to give the DHCP status of network adapters. Users will need to update their

Title: Assuria Auditor AutoUpdate #105 released

Number: 10 / 06

Date: 28 February 2010

inventory baselines to accommodate this new data.

Security Content Updates

Security content based on newly published vendor security bulletins (or similar) is included for the agents listed below:

- o HPUX 11.00, 11.11, 11.23, 11.31 (PA-RISC)
- o HPUX 11.23, 11.31 (Itanium)
- o IBM AIX 4.3.3, 5.1, 5.2, 5.3
- o IBM AIX 6.1
- o Microsoft Windows 2000 (Server and Professional)
- o Microsoft Windows Server 2003
- o Microsoft Windows Server 2008
- o Microsoft Windows Vista
- o Novell SUSE Enterprise Linux 9 (x86)
- o Novell SUSE Enterprise Linux 10 (x86)
- o Red Hat Enterprise Linux 3, 4, 5
- o Sun Solaris 8
- o Sun Solaris 9
- o Sun Solaris 10 (SPARC)
- o VMware ESX 3

Console update

- o Update Database

- o Update Files
 - bin/tcl/IndexedResults.tbc

- o Policy Navigators for:
 - HPUX 11.00, 11.11, 11.23, 11.31 (PA-RISC)
 - HPUX 11.23, 11.31 (Itanium)
 - IBM AIX 4.3.3, 5.1, 5.2, 5.3
 - IBM AIX 6.1
 - Microsoft Windows 2000 (Server and Professional)
 - Microsoft Windows Server 2003
 - Microsoft Windows Server 2008
 - Microsoft Windows Vista
 - Novell SUSE Enterprise Linux 9 (x86)
 - Novell SUSE Enterprise Linux 10 (x86)
 - Red Hat Enterprise Linux 3, 4, 5
 - Sun Solaris 8
 - Sun Solaris 9
 - Sun Solaris 10 (SPARC)
 - Sun Solaris 10 (X86)
 - VMware ESX 3

Agent updates

HP 11.00, 11.11, 11.23, 11.31 (PA-RISC)

- o New Checks
 - ntp-running
 - ntp-servers

Title: Assuria Auditor AutoUpdate #105 released

Number: 10 / 06

Date: 28 February 2010

- ports-listening
- server-using-dhcp-client

o Updated Checks

- once-only-11
- oo-smver

o Updated Files

- bin/procs/proc_inventory.tcl

o Updated Policies

- Initial-2
- Initial-All
- Maintenance-2
- Maintenance-All

o Updated Patch Databases

- bin/patch_HP-UX.data
- bin/patch_HP-UX.ref

o Auto Update Files

- rulesets/unarchivePolicy
- signatures/rulesets/unarchivePolicy.sgn
- lib/xpud3_105.zip
- lib/xpud3_105.sgn
- etc/update.ini

**HP 11.23, 11.31
(Itanium)**

o New Checks

- ntp-running
- ntp-servers
- ports-listening
- server-using-dhcp-client

o Updated Checks

- once-only-11
- oo-smver

o Updated Files

- bin/procs/proc_inventory.tcl

o Updated Policies

- Initial-2
- Initial-All
- Maintenance-2
- Maintenance-All

o Updated Patch Databases

- bin/patch_HP-UX.data

Title: Assuria Auditor AutoUpdate #105 released

Number: 10 / 06

Date: 28 February 2010

- bin/patch_HP-UX.ref

- o Auto Update Files

- rulesets/unarchivePolicy
- signatures/rulesets/unarchivePolicy.sgn
- lib/xpud3_105.zip
- lib/xpud3_105.sgn
- etc/update.ini

**IBM AIX 4.3.3, 5.1,
5.2, 5.3**

- o New Checks

- aix-20100113-OpenSSL-session-renegotiation-fix
- aix-IZ56203-fix
- aix-IZ56204-fix
- aix-IZ56205-fix
- aix-IZ56206-fix
- aix-IZ56311-fix
- aix-IZ56312-fix
- aix-IZ56313-fix
- aix-IZ56314-fix
- aix-IZ56315-fix
- aix-IZ56316-fix
- aix-IZ56317-fix
- aix-IZ56318-fix
- aix-IZ56697-fix
- aix-IZ56837-fix
- aix-IZ61324-fix
- ntp-running
- ntp-servers
- ports-listening
- server-using-dhcp-client

- o Updated Checks

- aix-IY89168-fix
- aix-IY93084-fix
- aix-IY94301-fix
- aix-IY94368-fix
- aix-IZ04133-fix
- aix-IY96095-fix
- aix-IY96101-fix
- aix-IY97257-fix
- once-only-11
- oo-smver

- o Updated Files

- bin/procs/proc_inventory.tcl

- o Updated Policies

Title: Assuria Auditor AutoUpdate #105 released

Number: 10 / 06

Date: 28 February 2010

- aix-fixes
- Initial-1
- Initial-2
- Initial-All
- Maintenance-1
- Maintenance-2
- Maintenance-All
- PatchChecks

o Auto Update Files

- rulesets/unarchivePolicy
- signatures/rulesets/unarchivePolicy.sgn
- lib/xpud3_105.zip
- lib/xpud3_105.sgn
- etc/update.ini

IBM AIX 6.1

o New Checks

- aix-20100113-OpenSSL-session-renegotiation-fix
- aix-IZ56203-fix
- aix-IZ56204-fix
- aix-IZ56205-fix
- aix-IZ56206-fix
- aix-IZ56311-fix
- aix-IZ56312-fix
- aix-IZ56313-fix
- aix-IZ56314-fix
- aix-IZ56315-fix
- aix-IZ56316-fix
- aix-IZ56317-fix
- aix-IZ56318-fix
- aix-IZ56697-fix
- aix-IZ56837-fix
- aix-IZ61324-fix
- ntp-running
- ntp-servers
- ports-listening
- server-using-dhcp-client

o Updated Checks

- aix-IY89168-fix
- aix-IY93084-fix
- aix-IY94301-fix
- aix-IY94368-fix
- aix-IY97257-fix
- aix-IY96095-fix
- aix-IY96101-fix
- aix-IZ04133-fix
- once-only-11

Title: Assuria Auditor AutoUpdate #105 released

Number: 10 / 06

Date: 28 February 2010

- oo-smver

- o Updated Files

- bin/procs/proc_inventory.tcl

- o Updated Policies

- Initial-2
 - Initial-All
 - Maintenance-2
 - Maintenance-All
 - PatchChecks

- o Auto Update Files

- rulesets/unarchivePolicy
 - signatures/rulesets/unarchivePolicy.sgn
 - lib/xpud3_105.zip
 - lib/xpud3_105.sgn
 - etc/update.ini

**Microsoft Windows
2000 (Server and
Professional)**

- o New Checks

- ntp-running
 - ntp-servers
 - ports-listening
 - server-using-dhcp-client
 - win-ms10kb971468-update
 - win-ms10kb975713-update
 - win-ms10kb977165-update
 - win-ms10kb977290-update
 - win-ms10kb978037-update
 - win-ms10kb978214-update
 - win-ms10kb978251-update
 - win-ms10kb978262-update

- o Updated Checks

- oo-smver

- o Updated Files

- bin/procs/proc_inventory.tcl
 - bin/procs/tools.tcl

- o Updated Policies

- Initial-1
 - Initial-2
 - Initial-All
 - Maintenance-1
 - Maintenance-2
 - Maintenance-All
 - PatchChecks

Title: Assuria Auditor AutoUpdate #105 released

Number: 10 / 06

Date: 28 February 2010

- versionChecks

- o Auto Update Files

- rulesets/unarchivePolicy
- signatures/rulesets/unarchivePolicy.sgn
- lib/xpud3_105.zip
- lib/xpud3_105.sgn
- etc/update.ini

**Microsoft Windows
Server 2003**

- o New Checks

- ntp-running
- ntp-servers
- ports-listening
- server-using-dhcp-client
- win-ms10kb971468-update
- win-ms10kb975713-update
- win-ms10kb977165-update
- win-ms10kb977290-update
- win-ms10kb978037-update
- win-ms10kb978214-update
- win-ms10kb978251-update
- win-ms10kb978262-update

- o Updated Checks

- oo-smver

- o Updated Files

- bin/procs/proc_inventory.tcl
- bin/procs/tools.tcl

- o Updated Policies

- Initial-1
- Initial-2
- Initial-All
- Maintenance-1
- Maintenance-2
- Maintenance-All
- PatchChecks
- versionChecks

- o Auto Update Files

- rulesets/unarchivePolicy
- signatures/rulesets/unarchivePolicy.sgn
- lib/xpud3_105.zip
- lib/xpud3_105.sgn
- etc/update.ini

Microsoft Windows

- o New Checks

Title: Assuria Auditor AutoUpdate #105 released

Number: 10 / 06

Date: 28 February 2010

Server 2008

- access-removable-media
- allow-loc-sys-null-ses-fallback
- allow-loc-sys-use-comp-ident
- allow-PKU2U-auth-requests
- anon-pipe-share-access
- anonymous-SAM
- audit-policy-overridden
- disable-credentials
- disable-password-change
- disconnect-idle-time
- eject-NTFS-media
- encrypt-secure-channel
- everyone-permissions
- forced-logoff
- install-printer-drivers
- kerberos-allowed-encryption
- key-protection
- LDAP-client-signing
- LDAP-server-signing
- machine-password-age
- machine-password-change
- NTLM-audit-authentication
- NTLM-audit-incoming-traffic
- NTLM-authentication
- NTLM-client-security
- NTLM-domain-server-exceptions
- NTLM-incoming-traffic
- NTLM-outgoing-traffic
- NTLM-remote-server-exceptions
- NTLM-server-security
- ntp-running
- ntp-servers
- ports-listening
- rc-automatic-logon
- rc-set-command
- remote-access-reg-paths
- remote-access-reg-sub-paths
- require-case-insensitivity
- require-sign-or-seal
- require-smart-card
- security-model-local-accounts
- server-using-dhcp-client
- sign-secure-channel
- smart-card-removal
- SPN-target-name-validation
- strong-session-key
- uac-admin-approval-mode
- uac-admin-as-standard-user

Title: Assuria Auditor AutoUpdate #105 released

Number: 10 / 06

Date: 28 February 2010

- uac-admin-elevation-prompt
- uac-codesignatures
- uac-elevate-secure-paths
- uac-enable-virtualization
- uac-installer-detection
- uac-user-elevation-prompt
- undock-without-logon
- unlock-authentication
- use-certificate-rules
- use-FIPS-algorithms
- user-display-when-locked
- win-ms10kb971468-update
- win-ms10kb974145-update
- win-ms10kb977165-update
- win-ms10kb977290-update
- win-ms10kb978214-update
- win-ms10kb978251-update
- win-ms10kb978262-update

o Updated Files

- bin/procs/proc_inventory.tcl
- bin/procs/tools.tcl

o Updated Policies

- Initial-1
- Initial-2
- Initial-4
- Initial-All
- Maintenance-1
- Maintenance-2
- Maintenance-5
- Maintenance-All
- PatchChecks

o Auto Update Files

- rulesets/unarchivePolicy
- signatures/rulesets/unarchivePolicy.sgn
- lib/xpud3_105.zip
- lib/xpud3_105.sgn
- etc/update.ini

**Microsoft Windows
Vista**

o New Checks

- access-removable-media
- ntp-running
- ntp-servers
- ports-listening
- server-using-dhcp-client
- win-ms10kb971468-update

Title: Assuria Auditor AutoUpdate #105 released

Number: 10 / 06

Date: 28 February 2010

- win-ms10kb974145-update
- win-ms10kb977165-update
- win-ms10kb978214-update
- win-ms10kb978251-update
- win-ms10kb978262-update

o Updated Files

- bin/procs/proc_inventory.tcl
- bin/procs/tools.tcl

o Updated Policies

- Initial-2
- Initial-All
- Maintenance-2
- Maintenance-All
- PatchChecks

o Auto Update Files

- rulesets/unarchivePolicy
- signatures/rulesets/unarchivePolicy.sgn
- lib/xpud3_105.zip
- lib/xpud3_105.sgn
- etc/update.ini

**Novell SUSE Enterprise
Linux 9 (x86)**

o New Checks

- ntp-running
- ntp-servers
- ports-listening
- server-using-dhcp-client
- SuSE-SA-2009-049
- SuSE-SA-2010-007
- SuSE-SA-2010-002
- SuSE-SA-2010-003
- SuSE-SA-2010-004
- SuSE-SA-2010-005
- SuSE-SA-2010-006
- SuSE-SA-2010-008
- SuSE-SA-2010-009

o Updated Checks

- once-only-11
- oo-smver
- SuSE-SA-2009-002
- SuSE-SA-2009-005
- SuSE-SA-2009-008
- SuSE-SA-2009-051
- SuSE-SA-2009-052
- SuSE-SA-2009-048

Title: Assuria Auditor AutoUpdate #105 released

Number: 10 / 06

Date: 28 February 2010

- SuSE-SA-2009-053
- SuSE-SA-2009-054
- SuSE-SA-2009-059
- SuSE-SA-2009-060
- SuSE-SA-2009-006
- SuSE-SA-2009-007

o Updated Files

- bin/procs/proc_inventory.tcl

o Updated policies

- Initial-1
- Initial-2
- Initial-All
- Maintenance-1
- Maintenance-2
- Maintenance-All
- PatchChecks
- ssa

o Auto Update Files

- rulesets/unarchivePolicy
- signatures/rulesets/unarchivePolicy.sgn
- lib/xpud3_105.zip
- lib/xpud3_105.sgn
- etc/update.ini

**Novell SUSE Enterprise
Linux 10 (x86)**

o New Checks

- ntp-running
- ntp-servers
- ports-listening
- server-using-dhcp-client
- SuSE-SA-2009-049
- SuSE-SA-2010-007
- SuSE-SA-2010-002
- SuSE-SA-2010-003
- SuSE-SA-2010-004
- SuSE-SA-2010-005
- SuSE-SA-2010-006
- SuSE-SA-2010-008
- SuSE-SA-2010-009

o Updated Checks

- once-only-11
- oo-smver
- SuSE-SA-2009-002
- SuSE-SA-2009-005
- SuSE-SA-2009-008

Title: Assuria Auditor AutoUpdate #105 released

Number: 10 / 06

Date: 28 February 2010

- SuSE-SA-2009-051
- SuSE-SA-2009-052
- SuSE-SA-2009-048
- SuSE-SA-2009-053
- SuSE-SA-2009-054
- SuSE-SA-2009-059
- SuSE-SA-2009-060
- SuSE-SA-2009-006
- SuSE-SA-2009-007

o Updated Files

- bin/procs/proc_inventory.tcl

o Updated policies

- Initial-1
- Initial-2
- Initial-All
- Maintenance-1
- Maintenance-2
- Maintenance-All
- PatchChecks
- ssa

o Auto Update Files

- rulesets/unarchivePolicy
- signatures/rulesets/unarchivePolicy.sgn
- lib/xpud3_105.zip
- lib/xpud3_105.sgn
- etc/update.ini

**Red Hat Enterprise
Linux 3, 4, 5**

o New Checks

- ntp-running
- ntp-servers
- ports-listening
- server-using-dhcp-client
- RHSA-2010-0029
- RHSA-2010-0037
- RHSA-2010-0038
- RHSA-2010-0039
- RHSA-2010-0040
- RHSA-2010-0044
- RHSA-2010-0053
- RHSA-2010-0054
- RHSA-2010-0060
- RHSA-2010-0061
- RHSA-2010-0062
- RHSA-2010-0076
- RHSA-2010-0046
- RHSA-2010-0079

Title: Assuria Auditor AutoUpdate #105 released
Number: 10 / 06 Date: 28 February 2010

o Updated Checks

- once-only-11
- oo-smver
- RHSA-2006-0140
- RHSA-2006-0156
- RHSA-2006-0160
- RHSA-2006-0163
- RHSA-2006-0177
- RHSA-2006-0184
- RHSA-2006-0194
- RHSA-2006-0199
- RHSA-2006-0200
- RHSA-2006-0207
- RHSA-2007-0014
- RHSA-2007-0021
- RHSA-2007-0062
- RHSA-2007-0073
- RHSA-2008-0005
- RHSA-2008-0006
- RHSA-2008-0008
- RHSA-2008-0038
- RHSA-2008-0039
- RHSA-2008-0055
- RHSA-2008-0103
- RHSA-2008-0104
- RHSA-2008-0105
- RHSA-2009-0014
- RHSA-2009-0057
- RHSA-2009-1504
- RHSA-2009-1500
- RHSA-2009-1505
- RHSA-2009-1513
- RHSA-2009-1522
- RHSA-2009-1528
- RHSA-2009-1530
- RHSA-2009-1531
- RHSA-2009-1541
- RHSA-2009-1548
- RHSA-2009-1550
- RHSA-2009-1642
- RHSA-2010-0019
- RHSA-2010-0020

o Updated Files

- bin/procs/proc_inventory.tcl

o Updated Policies

- Initial-1
- Initial-2

Title: Assuria Auditor AutoUpdate #105 released

Number: 10 / 06

Date: 28 February 2010

- Initial-All
- Maintenance-1
- Maintenance-2
- Maintenance-All
- PatchChecks
- rrsa

- o Auto Update Files
 - rulesets/unarchivePolicy
 - signatures/rulesets/unarchivePolicy.sgn
 - lib/xpud3_105.zip
 - lib/xpud3_105.sgn
 - etc/update.ini

Sun Solaris 8

- o New Checks
 - ntp-running
 - ntp-servers
 - ports-listening
 - server-using-dhcp-client
- o Updated Checks
 - once-only-11
 - oo-smver
- o Updated Files
 - bin/procs/proc_inventory.tcl
- o Updated Policies
 - Initial-2
 - Initial-All
 - Maintenance-2
 - Maintenance-All
- o Updated Patch Databases
 - bin/patch_Solaris.data
 - bin/patch_Solaris.ref
- o Auto Update Files
 - rulesets/unarchivePolicy
 - signatures/rulesets/unarchivePolicy.sgn
 - lib/xpud3_105.zip
 - lib/xpud3_105.sgn
 - etc/update.ini

Sun Solaris 9

- o New Checks
 - ntp-running
 - ntp-servers
 - ports-listening

Title: Assuria Auditor AutoUpdate #105 released

Number: 10 / 06

Date: 28 February 2010

- server-using-dhcp-client

- o Updated Checks

- once-only-11
- oo-smver

- o Updated Files

- bin/procs/proc_inventory.tcl

- o Updated Policies

- Initial-2
- Initial-All
- Maintenance-2
- Maintenance-All

- o Updated Patch Databases

- bin/patch_Solaris.data
- bin/patch_Solaris.ref

- o Auto Update Files

- rulesets/unarchivePolicy
- signatures/rulesets/unarchivePolicy.sgn
- lib/xpud3_105.zip
- lib/xpud3_105.sgn
- etc/update.ini

Sun Solaris 10 (SPARC)

- o New Checks

- ntp-running
- ntp-servers
- ports-listening
- server-using-dhcp-client

- o Updated Checks

- once-only-11
- oo-smver

- o Updated Files

- bin/procs/proc_inventory.tcl

- o Updated Policies

- Initial-2
- Initial-All
- Maintenance-2
- Maintenance-All

- o Updated Patch Databases

- bin/patch_Solaris.data
- bin/patch_Solaris.ref

Title: Assuria Auditor AutoUpdate #105 released

Number: 10 / 06

Date: 28 February 2010

- o Auto Update Files
 - rulesets/unarchivePolicy
 - signatures/rulesets/unarchivePolicy.sgn
 - lib/xpud3_105.zip
 - lib/xpud3_105.sgn
 - etc/update.ini

**Sun Solaris 10
(x86)**

- o Updated Patch Databases
 - bin/patch_Solaris.data
 - bin/patch_Solaris.ref

- o Auto Update Files
 - rulesets/unarchivePolicy
 - signatures/rulesets/unarchivePolicy.sgn
 - lib/xpud3_105.zip
 - lib/xpud3_105.sgn
 - etc/update.ini

VMware ESX 3.5

- o New Checks
 - ntp-running
 - ntp-servers
 - ports-listening
 - server-using-dhcp-client

- o Updated Files
 - bin/procs/proc_inventory.tcl

- o Updated Policies
 - Initial-2
 - Initial-All
 - Maintenance-2
 - Maintenance-All

- o Updated Checks
 - once-only-11
 - oo-smver

- o Auto Update Files
 - rulesets/unarchivePolicy
 - signatures/rulesets/unarchivePolicy.sgn
 - lib/xpud3_105.zip
 - lib/xpud3_105.sgn
 - etc/update.ini