

**Title: Assuria Auditor AutoUpdate #112 released**

**Number: 10-19**

**Date: 30<sup>th</sup> July 2010**

**Title Assuria Auditor AutoUpdate #112 released**

### **Introduction**

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

### **Contents**

#### **Inventory Baseline Enhancements for Microsoft Windows platforms**

The folders beneath the program files folder on Microsoft Windows platforms are now baselined with their creation date. A new tab called 'Program\_Files' can be found in the Assuria console Baselines ->Inventory screen for an Agent once this update has been applied to the agent and the Inventory Baseline updated.

Please note that existing Inventory Baselines for your Microsoft Windows agents will need to be updated once this update has been applied. Failure to do will result in folders added baseline vulnerabilities being reported (when 'CheckAllbaselines' or 'ChecksInventoryBaseline' is run) for each and every folder under program files for that agent.

#### **Security Content Updates**

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

- HPUX 11.00, 11.11, 11.23, 11.31 (PA-RISC)
- HPUX 11.23, 11.31 (Itanium)
- Novell SUSE Linux Enterprise Server 9 (x86)
- Novell SUSE Linux Enterprise Server 10 (x86)
- Microsoft Windows 2000 (Server and Professional)
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 R2
- Microsoft Windows Vista
- Red Hat Enterprise Linux 3, 4, 5
- Sun Solaris 8
- Sun Solaris 9
- Sun Solaris 10 (SPARC)
- Sun Solaris 10 (X86)
- VMware ESX 3

**Title: Assuria Auditor AutoUpdate #112 released**  
**Number: 10-19 Date: 30<sup>th</sup> July 2010**

**Console update**

- o Update Files
  - etc/masteragentvariables.ini
  - lib/DbImport/dbresimport.tcl
  - scripts/create\_standards\_report
  
- o Update Database
  
- 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 Server 2008 R2
  - 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**

Updates are included for the following agents:

- 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 Server 2008 R2
- o Microsoft Windows Vista

**Title: Assuria Auditor AutoUpdate #112 released**  
**Number: 10-19 Date: 30<sup>th</sup> July 2010**

- o Novell SUSE Linux Enterprise Server 9 (x86)
- o Novell SUSE Linux Enterprise Server 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

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

- o Updated Checks
  - ntp-running
  - ports-listening
- o Updated Files
  - bin/procs/proc\_inventory.tcl
- 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\_112.zip
  - lib/xpud3\_112.sgn
  - etc/update.ini

**HP 11.23, 11.31  
(Itanium)**

- o Updated Checks
  - ntp-running
  - ports-listening
- o Updated Files
  - bin/procs/proc\_inventory.tcl
- o Updated Patch Databases
  - bin/patch\_HP-UX.data
  - bin/patch\_HP-UX.ref

**Title: Assuria Auditor AutoUpdate #112 released**

**Number: 10-19**

**Date: 30<sup>th</sup> July 2010**

o Auto Update Files

- rulesets/unarchivePolicy
- signatures/rulesets/unarchivePolicy.sgn
- lib/xpud3\_112.zip
- lib/xpud3\_112.sgn
- etc/update.ini

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

o New Checks

- aix-IY86038-fix
- aix-IY86037-fix
- aix-20100602-OpenSSL-record-of-death-fix
- aix-20091104-PowerHA-godm-port-fix
- aix-20090804-libC-environment-var-fix
- aix-20090511-OpenSSL-cmsverify-fix
- aix-20070403-Kerberos-kadmind-fix
- aix-IZ75369-fix
- aix-IZ75440-fix
- aix-IZ75465-fix
- aix-OpenSSH-X11-plaintext-fix
- aix-20090629-OpenSSL-dlts-fix
- aix-20080221-Pegasus-CIM-Server-fix

o Updated Checks

- aix-20080205-OpenSSH-trusted-cookie-fix
- aix-20080521-OpenSSH-sshrc-fix
- aix-20100113-OpenSSL-session-renegotiation-fix
- ntp-running
- ports-listening

o Updated Files

- bin/procs/proc\_inventory.tcl

o Updated Policies

- PatchChecks

o Auto Update Files

- rulesets/unarchivePolicy

**Title: Assuria Auditor AutoUpdate #112 released**  
**Number: 10-19 Date: 30<sup>th</sup> July 2010**

- signatures/rulesets/unarchivePolicy.sgn
- lib/xpud3\_112.zip
- lib/xpud3\_112.sgn
- etc/update.ini

## **IBM AIX 6.1**

- o New Checks
  - aix-IY86038-fix
  - aix-IY86037-fix
  - aix-20100602-OpenSSL-record-of-death-fix
  - aix-20091104-PowerHA-godm-port-fix
  - aix-20090804-libC-environment-var-fix
  - aix-20090511-OpenSSL-cmsverify-fix
  - aix-20070403-Kerberos-kadmind-fix
  - aix-IZ75369-fix
  - aix-IZ75440-fix
  - aix-IZ75465-fix
  - aix-OpenSSH-X11-plaintext-fix
  - aix-20090629-OpenSSL-dlts-fix
  - aix-20080221-Pegasus-CIM-Server-fix
- o Updated Checks
  - aix-20080205-OpenSSH-trusted-cookie-fix
  - aix-20080521-OpenSSH-sshrc-fix
  - aix-20100113-OpenSSL-session-renegotiation-fix
  - file-all-04
  - file-all-05
  - file-cfg-14
  - file-cfg-15
  - file-cronat-03
  - file-exrc-03
  - file-inet-01
  - file-uucp-01
  - file-filsys-02
  - ntp-running
  - ports-listening
- o Updated Files

**Title: Assuria Auditor AutoUpdate #112 released**

**Number: 10-19**

**Date: 30<sup>th</sup> July 2010**

- bin/procs/proc\_inventory.tcl

- o Updated Policies

- PatchChecks

- o Auto Update Files

- rulesets/unarchivePolicy

- signatures/rulesets/unarchivePolicy.sgn

- lib/xpud3\_112.zip

- lib/xpud3\_112.sgn

- etc/update.ini

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

- o New Checks

- win-ms10kb978212-update

- win-ms10kb982335-update

- o Updated Checks

- ports-listening

- win-ms08kb941693-update

- win-ms09kb975539-update

- win-no-security-updates

- o Updated Files

- bin/procs/proc\_inventory.tcl

- bin/procs/tools.tcl

- o Updated Policies

- PatchChecks

- o Auto Update Files

- rulesets/unarchivePolicy

- signatures/rulesets/unarchivePolicy.sgn

- lib/xpud3\_112.zip

- lib/xpud3\_112.sgn

- etc/update.ini

**Microsoft Windows**

- o New Checks

© Copyright Assuria Limited 2010. All rights reserved.

Page 6 of 20

**Title: Assuria Auditor AutoUpdate #112 released**  
**Number: 10-19 Date: 30<sup>th</sup> July 2010**

**Server 2003**

- win-ms10kb2229593-update
- win-ms10kb978212-update
- win-ms10kb982335-update

o Updated Checks

- ports-listening
- win-ms08kb941693-update
- win-ms09kb975539-update
- win-no-security-updates

o Updated Files

- bin/procs/proc\_inventory.tcl
- bin/procs/tools.tcl

o Updated Policies

- PatchChecks

o Auto Update Files

- rulesets/unarchivePolicy
- signatures/rulesets/unarchivePolicy.sgn
- lib/xpud3\_112.zip
- lib/xpud3\_112.sgn
- etc/update.ini

**Microsoft Windows  
Server 2008**

o New Checks

- win-ms10kb978212-update
- win-ms10kb982335-update
- win-no-security-updates

o Updated Checks

- ports-listening
- win-ms08kb941693-update
- win-ms09kb974455-update
- win-ms09kb975539-update
- win-ms09kb976325-update
- win-ms10kb978207-update
- win-ms10kb980182-update

**Title: Assuria Auditor AutoUpdate #112 released**

**Number: 10-19**

**Date: 30<sup>th</sup> July 2010**

- win-ms10kb982381-update

- o Updated Files

- bin/procs/proc\_inventory.tcl
- bin/procs/tools.tcl

- o Updated Policies

- PatchChecks

- o Auto Update Files

- rulesets/unarchivePolicy
- signatures/rulesets/unarchivePolicy.sgn
- lib/xpud3\_112.zip
- lib/xpud3\_112.sgn
- etc/update.ini

**Microsoft Windows  
Server 2008 R2**

- o New Checks

- adobe-flash-player-apsb10-07-update
- adobe-reader-apsb10-07-update
- adobe-reader-apsb10-09-update
- win-ms10kb2027452-update
- win-ms10kb2032276-update
- win-ms10kb978212-update
- win-ms10kb979559-update
- win-ms10kb979902-update
- win-ms10kb980195-update
- win-ms10kb980218-update
- win-ms10kb981343-update
- win-ms10kb982335-update
- win-ms10kb982381-update
- win-ms10kb982666-update
- win-ms10kb983235-update

- o Updated Checks

- ports-listening
- win-ms08kb941693-update
- win-ms09kb975539-update

**Title: Assuria Auditor AutoUpdate #112 released**

**Number: 10-19**

**Date: 30<sup>th</sup> July 2010**

- win-no-security-updates

- o Updated Files

- bin/procs/proc\_inventory.tcl

- bin/procs/tools.tcl

- lib/verify/Verify10.dll

- lib/verify/Verify10.dll.sgn

- o Updated Policies

- PatchChecks

- o Auto Update Files

- rulesets/unarchivePolicy

- signatures/rulesets/unarchivePolicy.sgn

- lib/xpud3\_112.zip

- lib/xpud3\_112.sgn

- etc/update.ini

**Microsoft Windows  
Vista**

- o New Checks

- win-ms10kb978212-update

- win-ms10kb982335-update

- o Updated Checks

- ports-listening

- win-ms08kb941693-update

- win-ms09kb974455-update

- win-ms09kb975539-update

- win-ms09kb976325-update

- win-ms10kb978207-update

- win-ms10kb980182-update

- win-ms10kb982381-update

- win-no-security-updates

- o Updated Files

- bin/procs/proc\_inventory.tcl

- bin/procs/tools.tcl

**Title: Assuria Auditor AutoUpdate #112 released**

**Number: 10-19**

**Date: 30<sup>th</sup> July 2010**

- o Updated Policies
  - PatchChecks

- o Auto Update Files
  - rulesets/unarchivePolicy
  - signatures/rulesets/unarchivePolicy.sgn
  - lib/xpud3\_112.zip
  - lib/xpud3\_112.sgn
  - etc/update.ini

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

- o New Checks
  - SuSE-SA-2009-027
  - SuSE-SA-2010-013
  - SuSE-SA-2010-020

- o Updated Checks
  - ntp-running
  - ports-listening
  - SuSE-SA-2010-025
  - SuSE-SA-2010-026
  - SuSE-SA-2010-027
  - SuSE-SA-2010-028
  - SuSE-SA-2010-030

- o Updated Files
  - bin/procs/proc\_inventory.tcl

- o Updated policies
  - PatchChecks

- o Auto Update Files
  - rulesets/unarchivePolicy
  - signatures/rulesets/unarchivePolicy.sgn
  - lib/xpud3\_112.zip
  - lib/xpud3\_112.sgn
  - etc/update.ini

**Title: Assuria Auditor AutoUpdate #112 released**

**Number: 10-19**

**Date: 30<sup>th</sup> July 2010**

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

- o New Checks
  - SuSE-SA-2009-027
  - SuSE-SA-2010-013
  - SuSE-SA-2010-020
  
- o Updated Checks
  - ntp-running
  - ports-listening
  - SuSE-SA-2010-025
  - SuSE-SA-2010-026
  - SuSE-SA-2010-027
  - SuSE-SA-2010-028
  - SuSE-SA-2010-030
  
- o Updated Files
  - bin/procs/proc\_inventory.tcl
  
- o Updated policies
  - PatchChecks
  
- o Auto Update Files
  - rulesets/unarchivePolicy
  - signatures/rulesets/unarchivePolicy.sgn
  - lib/xpud3\_112.zip
  - lib/xpud3\_112.sgn
  - etc/update.ini

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

- o New Checks
  - RHSA-2010-0457
  - RHSA-2010-0458
  - RHSA-2010-0459
  - RHSA-2010-0464
  - RHSA-2010-0470
  - RHSA-2010-0474
  - RHSA-2010-0475
  - RHSA-2010-0488

**Title: Assuria Auditor AutoUpdate #112 released**

**Number: 10-19**

**Date: 30<sup>th</sup> July 2010**

- RHSA-2010-0489
- RHSA-2010-0490
- RHSA-2010-0499
- RHSA-2010-0500
- RHSA-2010-0501
- RHSA-2010-0503
- RHSA-2010-0504
- RHSA-2010-0505
- RHSA-2010-0518
- RHSA-2010-0520
- RHSA-2010-0519

o Updated Checks

- ntp-running
- ports-listening
- RHSA-2007-0384
- RHSA-2007-0395
- RHSA-2007-0403
- RHSA-2007-0436
- RHSA-2007-0465
- RHSA-2007-0488
- RHSA-2007-0497
- RHSA-2007-0501
- RHSA-2007-0509
- RHSA-2007-0510
- RHSA-2007-0533
- RHSA-2007-0534
- RHSA-2007-0556
- RHSA-2007-0562
- RHSA-2008-0497
- RHSA-2008-0502
- RHSA-2008-0503
- RHSA-2008-0504
- RHSA-2008-0508
- RHSA-2008-0519
- RHSA-2008-0522
- RHSA-2008-0537

**Title: Assuria Auditor AutoUpdate #112 released**

**Number: 10-19**

**Date: 30<sup>th</sup> July 2010**

- RHSA-2009-0476
- RHSA-2009-1106
- RHSA-2009-1107
- RHSA-2009-1108
- RHSA-2009-1109
- RHSA-2009-1125
- RHSA-2009-1126
- RHSA-2009-1132
- RHSA-2009-1148
- RHSA-2010-0140
- RHSA-2010-0153
- RHSA-2010-0154
- RHSA-2010-0155
- RHSA-2010-0162
- RHSA-2010-0163
- RHSA-2010-0164
- RHSA-2010-0165
- RHSA-2010-0166
- RHSA-2010-0167
- RHSA-2010-0168
- RHSA-2010-0173
- RHSA-2010-0175
- RHSA-2010-0271
- RHSA-2010-0273
- RHSA-2010-0332
- RHSA-2010-0333
- RHSA-2010-0337
- RHSA-2010-0338
- RHSA-2010-0339
- RHSA-2010-0383
- RHSA-2010-0399
- RHSA-2010-0400
- RHSA-2010-0401
- RHSA-2010-0449

o Updated Files

- bin/procs/proc\_inventory.tcl

**Title: Assuria Auditor AutoUpdate #112 released**  
**Number: 10-19 Date: 30<sup>th</sup> July 2010**

- o Updated Policies
  - PatchChecks
  
- o Auto Update Files
  - rulesets/unarchivePolicy
  - signatures/rulesets/unarchivePolicy.sgn
  - lib/xpud3\_112.zip
  - lib/xpud3\_112.sgn
  - etc/update.ini

**Sun Solaris 8**

- o Updated Checks
  - ntp-running
  - ports-listening
  
- o Updated Files
  - bin/procs/proc\_inventory.tcl
  - bin/procs/tools.tcl
  
- o Updated Patch Databases
  - bin/patch\_Solaris.data
  - bin/patch\_Solaris.ref
  
- o Auto Update Files
  - rulesets/unarchivePolicy
  - signatures/rulesets/unarchivePolicy.sgn
  - lib/xpud3\_112.zip
  - lib/xpud3\_112.sgn
  - etc/update.ini

**Sun Solaris 9**

- o Updated Checks
  - ntp-running
  - ports-listening
  
- o Updated Files
  - bin/procs/proc\_inventory.tcl
  - bin/procs/tools.tcl

**Title: Assuria Auditor AutoUpdate #112 released**

**Number: 10-19**

**Date: 30<sup>th</sup> July 2010**

- o Updated Patch Databases
  - bin/patch\_Solaris.data
  - bin/patch\_Solaris.ref

- o Auto Update Files
  - rulesets/unarchivePolicy
  - signatures/rulesets/unarchivePolicy.sgn
  - lib/xpud3\_112.zip
  - lib/xpud3\_112.sgn
  - etc/update.ini

**Sun Solaris 10  
(SPARC)**

- o Updated Checks
  - ntp-running
  - ports-listening
- o Updated Files
  - bin/procs/ty\_textdata.tcl

- o Updated Patch Databases
  - bin/patch\_Solaris.data
  - bin/patch\_Solaris.ref

- o Auto Update Files
  - rulesets/unarchivePolicy
  - signatures/rulesets/unarchivePolicy.sgn
  - lib/xpud3\_112.zip
  - lib/xpud3\_112.sgn
  - etc/update.ini

**Sun Solaris 10  
(x86)**

- o New Checks
  - inventory-added
  - inventory-changed
  - inventory-deleted
  - ip-addr-not-in-range
  - ntp-running
  - ntp-servers

**Title: Assuria Auditor AutoUpdate #112 released**

**Number: 10-19**

**Date: 30<sup>th</sup> July 2010**

- oo-basic-security
- oo-defpwd-dictiondir
- oo-defpwd-dictionlist
- oo-defpwd-history
- oo-defpwd-maxrepeats
- oo-defpwd-maxweeks
- oo-defpwd-minalpha
- oo-defpwd-mindiff
- oo-defpwd-mindigit
- oo-defpwd-minlower
- oo-defpwd-minnonalpha
- oo-defpwd-minspecial
- oo-defpwd-minupper
- oo-defpwd-minweeks
- oo-defpwd-namecheck
- oo-defpwd-passlength
- oo-defpwd-warnweeks
- oo-defpwd-whitespace
- oo-inventory-1-0-devices
- oo-inventory-2-0-cpu
- oo-inventory-3-0-disks
- oo-inventory-4-0-model
- oo-inventory-5-0-network-adapter
- oo-inventory-active-ports
- oo-inventory-active-package
- package-add
- port-listening
- refreshFileBaseline
- server-using-dhcp-client
- tdfc-md5
- tdfc-user-profile-exist
- updateInventoryBaseline
- updateVmconfigBaseline
- vmconfig-devices-added
- vmconfig-devices-changed
- vmconfig-devices-deleted
- vmconfig-general-added

**Title: Assuria Auditor AutoUpdate #112 released**

**Number: 10-19**

**Date: 30<sup>th</sup> July 2010**

- vmconfig-general-changed
- vmconfig-general-deleted
- vmconfig-hardware-added
- vmconfig-hardware-changed
- vmconfig-hardware-deleted
- vmconfig-options-added
- vmconfig-options-changed
- vmconfig-options-deleted
- xpu-integrity-summary

o Updated Checks

- apache-default-content
- AS-Diagnostic-basic
- AS-Diagnostic-env
- AS-Diagnostic-globals
- AS-Diagnostic-users
- bind-enabled
- bind-opt-rr-dos
- bind-sig-rr-bo
- file-cfg-10
- frozen-file-01-log
- frozen-file-02-log
- frozen-file-03-log
- frozen-file-04-log
- frozen-file-05-log
- frozen-file-06-log
- frozen-file-07-log
- frozen-file-08-log
- frozen-file-09-log
- frozen-file-11-log
- ftp-wrapped
- lpd-wrapped
- ntp-running
- once-only-11
- once-only-107
- oo-smver
- ports-listening

**Title: Assuria Auditor AutoUpdate #112 released**

**Number: 10-19**

**Date: 30<sup>th</sup> July 2010**

- rc-command-groupwritable
- rc-command-missing
- rc-command-owner
- rc-command-worldwritable
- rservice-exec-wrapped
- rservice-login-wrapped
- rservice-shell-wrapped
- rtrust-remote-root
- sendmail-daemon-enabled
- user-40
- user-homedir-gw
- xpu-integrity

o New Files

- bin/procs/procs\_inventory.tcl
- bin/procs/proc\_vmconfig.tcl

o Updated Files

- adm/config/sysscan\_config
- bin/checker
- bin/get\_security\_patches.tcl
- bin/procs/procs\_packages.tcl
- bin/procs/tools.tcl
- bin/procs/ty\_textdata.tcl
- etc/agentinfo

o New Policies

- AS-Diagnostics
- CheckAllBaselines
- CheckFileBaseline
- CheckFilesLogBaseline
- CheckGroupBaseline
- CheckInventoryBaseline
- CheckPackageBaseline
- CheckTrustedHostsBaseline
- CheckUserBaseline
- CheckVmconfigBaseline

**Title: Assuria Auditor AutoUpdate #112 released**

**Number: 10-19**

**Date: 30<sup>th</sup> July 2010**

- frozenfileslog
- Inventory
- PatchChecks
- RefreshAllBaselines
- RefreshFileBaseline
- RefreshGroupBaseline
- RefreshInventoryBaseline
- RefreshPackageBaseline
- RefreshTrustedHostsBaseline
- RefreshUserBaseline
- RefreshVmconfigBaseline
- UpdateInventoryBaseline
- UpdateVmconfigBaseline
- xpu-integrity-summary

o Updated Policies

- Initial-1
- Initial-2
- Initial-3
- Maintenance-1
- Maintenance-2
- Maintenance-4
- Maintenance-All
- SANS\_Top\_20
- security-patches
- sys-cfgs
- sys-defs
- xpu-integrity

o Updated Patch Databases

- bin/patch\_Solaris.data
- bin/patch\_Solaris.ref

o Auto Update Files

- rulesets/unarchivePolicy
- signatures/rulesets/unarchivePolicy.sgn
- lib/xpud3\_112.zip

**Title: Assuria Auditor AutoUpdate #112 released**

**Number: 10-19**

**Date: 30<sup>th</sup> July 2010**

- lib/xpud3\_112.sgn
- etc/update.ini

**VMware ESX 3.5**

- o New Checks
  - ESX350-201006408-SG
  - ESX350-201006407-SG
  - ESX350-201006405-SG
  - ESX350-201006406-SG
  - ESX350-201006401-SG
- o Updated Checks
  - ESX350-200808413-SG
  - ntp-running
  - ports-listening
- o Updated Files
  - bin/procs/proc\_inventory.tcl
- o Updated Policies
  - PatchChecks
- o Auto Update Files
  - rulesets/unarchivePolicy
  - signatures/rulesets/unarchivePolicy.sgn
  - lib/xpud3\_112.zip
  - lib/xpud3\_112.sgn
  - etc/update.ini