

Title: Assuria Auditor AutoUpdate #100 released
Number: 104 **Date: 31 October 2009**

Title. Assuria Auditor AutoUpdate #100 released

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

Contents

USB usage A new USB forensics check has been added for Microsoft Windows 2003, 2008 and Vista. This report displays USB device usage held in the Windows registry. Policies Initial-1, Initial-All, Maintenance-1 and Maintenance-All are affected by this change.

Autorun New checks have been introduced to check for 'autorun' on Windows, and the existing 'autorun' check retired. Policies sys_info, Initial-5, Initial-All, Maintenance-3 and Maintenance-All are affected by this change.

Other changes The console splash screen has been updated.

A bug has been fixed in the display of policies when updating sessions with class level '@' entries.

The error handling of multiple concurrent database purge by date sessions has been improved.

New Unix / Linux configuration checks Some new Unix / Linux configuration checks are included for the agents listed below:

HP HP-UX 11.00, 11.11, 11.23, 11.31 (PA-RISC)
HP HP-UX 11.23, 11.31 (Itanium)
IBM AIX 4.3.3, 5.1, 5.2, 5.3
IBM AIX 6.1
Novell SUSE Enterprise Linux 9 (x86)
Novell SUSE Enterprise Linux 10 (x86)
Red Hat Enterprise Linux 3, 4, 5
Sun Solaris 9
Sun Solaris 10 (SPARC)

This introduces checking for missing user profiles, use of MD5 for password encryption (Red Hat and Sun only), the installation of the basic security component (HP, Novell and Sun only), and the

Title: Assuria Auditor AutoUpdate #100 released

Number: 104

Date: 31 October 2009

restriction of root login to the system console (HP only). Policies sys-cfgs, Initial-1, Initial-All, Maintenance-1 and Maintenance-All are affected by this change.

Security Content Updates

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

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

Console update

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 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)
- VMware ESX 3

o Updated Files

- bin/tcl/db.tbc
- bin/tcl/file.tbc
- bin/tcl/startup.tbc
- etc/images/splash.gif

Title: Assuria Auditor AutoUpdate #100 released

Number: 104

Date: 31 October 2009

- Store/config/reporter/styles/Multi-Session/Executive/Scans Summary Sorted by Host.html.xsl
- Store/config/reporter/styles/Multi-Session/Executive/Scans Summary Sorted by Host.pdf.xsl
- Store/config/reporter/styles/Multi-Session/Executive/Scans Summary Sorted by Vulnerability.html.xsl
- Store/config/reporter/styles/Multi-Session/Executive/Scans Summary Sorted by Vulnerability.pdf.xsl
- Store/config/reporter/templates/Multi-Session/Executive/Scans Summary Sorted by Host.xml
- Store/config/reporter/templates/Multi-Session/Executive/Scans Summary Sorted by Vulnerability.xml

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 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)

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

- o New Checks
 - oo-basic-security
 - oo-securetty-console
 - tdfc-user-profile-exist
- o Updated Policies
 - Initial-1
 - Initial-All
 - Maintenance-1
 - Maintenance-All
 - sys-cfgs
- o Updated Patch Databases
 - bin/patch_HP-UX.data
 - bin/patch_HP-UX.ref

Title: Assuria Auditor AutoUpdate #100 released

Number: 104

Date: 31 October 2009

- o Auto Update Files
 - rulesets/unarchivePolicy
 - signatures/rulesets/unarchivePolicy.sgn
 - lib/xpud3_99.zip
 - lib/xpud3_99.sgn
 - etc/update.ini

- HP 11.23, 11.31 (Itanium)**
 - o New Checks
 - oo-basic-security
 - oo-securetty-console
 - tdfc-user-profile-exist

 - o Updated Policies
 - Initial-1
 - Initial-All
 - Maintenance-1
 - Maintenance-All
 - sys-cfgs

 - 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_99.zip
 - lib/xpud3_99.sgn
 - etc/update.ini

- IBM AIX 4.3.3, 5.1, 5.2, 5.3**
 - o New Checks
 - aix-IZ02983-fix
 - aix-IZ02538-fix
 - aix-IY97338-fix
 - aix-IY96277-fix
 - aix-IY98532-fix
 - aix-IZ52848-fix
 - aix-IZ52849-fix
 - aix-IZ52850-fix
 - aix-IZ52851-fix
 - aix-IZ49096-fix
 - aix-IZ49278-fix
 - aix-IZ50399-fix
 - aix-IZ50444-fix
 - aix-IZ50496-fix
 - aix-IZ49024-fix
 - tdfc-user-profile-exist

Title: Assuria Auditor AutoUpdate #100 released

Number: 104

Date: 31 October 2009

- o Updated Checks
 - aix-IY89434-fix
 - aix-IY89512-fix
 - aix-IY88641-fix
 - aix-IY88642-fix
 - aix-IY88566-fix
 - aix-IY88615-fix
 - aix-IY88681-fix
 - aix-IY88735-fix
 - aix-IY88699-fix
 - aix-IY88722-fix
 - aix-IY76102-fix
 - aix-IY76483-fix
 - aix-IY88687-fix
 - aix-IY88688-fix
 - aix-IY88818-fix
 - aix-IY88820-fix
 - aix-IY88565-fix
 - aix-IY88614-fix
 - aix-IY87894-fix
 - aix-IY87943-fix
 - aix-IZ01134-fix
 - aix-IZ01135-fix
 - aix-IY94761-fix
 - aix-IY94739-fix
 - aix-IY97309-fix
 - aix-IY98819-fix
 - aix-IY98804-fix
 - aix-IZ50445-fix
 - aix-IZ50447-fix
 - aix-IZ50500-fix
 - aix-IZ50517-fix
 - aix-IZ50121-fix
 - aix-IZ50129-fix
 - aix-IZ50139-fix
 - aix-IZ52842-fix

- o Updated Policies
 - Initial-1
 - Initial-All
 - Maintenance-1
 - Maintenance-All
 - sys-cfgs

- o Updated Policies
 - aix-fixes
 - Initial-1

Title: Assuria Auditor AutoUpdate #100 released
Number: 104 Date: 31 October 2009

- Initial-All
- Maintenance-1
- Maintenance-All

o Auto Update Files

- rulesets/unarchivePolicy
- signatures/rulesets/unarchivePolicy.sgn
- lib/xpud3_100.zip
- lib/xpud3_100.sgn
- etc/update.ini

IBM AIX 6.1

o New Checks

- aix-IZ02983-fix
- aix-IZ02538-fix
- aix-IY97338-fix
- aix-IY96277-fix
- aix-IY98532-fix
- aix-IZ52848-fix
- aix-IZ52849-fix
- aix-IZ52850-fix
- aix-IZ52851-fix
- aix-IZ49096-fix
- aix-IZ49278-fix
- aix-IZ50399-fix
- aix-IZ50444-fix
- aix-IZ50496-fix
- aix-IZ49024-fix
- tdfc-user-profile-exist

o Updated Checks

- aix-IY89434-fix
- aix-IY89512-fix
- aix-IY88641-fix
- aix-IY88642-fix
- aix-IY88566-fix
- aix-IY88615-fix
- aix-IY88681-fix
- aix-IY88735-fix
- aix-IY88699-fix
- aix-IY88722-fix
- aix-IY76102-fix
- aix-IY76483-fix
- aix-IY88687-fix
- aix-IY88688-fix
- aix-IY88818-fix
- aix-IY88820-fix
- aix-IY88565-fix
- aix-IY88614-fix

Title: Assuria Auditor AutoUpdate #100 released
Number: 104 **Date: 31 October 2009**

- aix-IY87894-fix
- aix-IY87943-fix
- aix-IZ01134-fix
- aix-IZ01135-fix
- aix-IY94761-fix
- aix-IY94739-fix
- aix-IY97309-fix
- aix-IY98819-fix
- aix-IY98804-fix
- aix-IZ50445-fix
- aix-IZ50447-fix
- aix-IZ50500-fix
- aix-IZ50517-fix
- aix-IZ50121-fix
- aix-IZ50129-fix
- aix-IZ50139-fix
- aix-IZ52842-fix

o Updated Policies

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

o Auto Update Files

- rulesets/unarchivePolicy
- signatures/rulesets/unarchivePolicy.sgn
- lib/xpud3_100.zip
- lib/xpud3_100.sgn
- etc/update.ini

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

o New Checks

- reg-autorun-03
- reg-autorun-04
- win-ms09kb957488-update
- win-ms09kb969059-update
- win-ms09kb971486-update
- win-ms09kb973525-update
- win-ms09kb973965-update
- win-ms09kb974112-update
- win-ms09kb974378-update
- win-ms09kb974455-update
- win-ms09kb974571-update
- win-ms09kb975254-update
- win-ms09kb975682-update
- win-no-dotnet-security-updates

Title: Assuria Auditor AutoUpdate #100 released
Number: 104 Date: 31 October 2009

o Updated Checks

- win-ms06kb917283-update
- win-ms06kb917953-update
- win-ms06kb922770-update
- win-ms07kb926122-update
- win-ms07kb931212-update
- win-ms07kb931768-update
- win-ms07kb933566-update
- win-ms07kb935966-update
- win-ms07kb937143-update
- win-ms07kb939653-update
- win-ms07kb941672-update
- win-ms07kb942615-update
- win-ms08kb941644-update
- win-ms08kb944533-update
- win-ms08kb946538-update
- win-ms08kb947864-update
- win-ms08kb948745-update
- win-ms08kb950759-update
- win-ms08kb953230-update
- win-ms08kb953235-update
- win-ms08kb953838-update
- win-ms08kb956390-update
- win-ms08kb957280-update
- win-ms09kb957638-update
- win-ms08kb958215-update
- win-ms08kb960714-update
- win-ms08kb961371-update
- win-ms09kb962238-update
- win-ms09kb963027-update
- win-ms09kb969897-update
- win-no-security-updates

o Updated Policies

- Initial-1
- Initial-5
- Initial-All
- Maintenance-1
- Maintenance-3
- Maintenance-All
- sys-info
- VersionChecks

o Auto Update Files

- rulesets/unarchivePolicy
- signatures/rulesets/unarchivePolicy.sgn
- lib/xpud3_100.zip
- lib/xpud3_100.sgn

Title: Assuria Auditor AutoUpdate #100 released
Number: 104 Date: 31 October 2009

- etc/update.ini

**Microsoft Windows
Server 2003**

- o Updated Files
 - bin/procs/tools.tcl
- o New Checks
 - load-user-vguids
 - reg-autorun-02
 - reg-autorun-03
 - reg-autorun-04
 - usb-report
 - win-ms09kb957488-update
 - win-ms09kb969059-update
 - win-ms09kb971486-update
 - win-ms09kb973525-update
 - win-ms09kb973965-update
 - win-ms09kb974112-update
 - win-ms09kb974378-update
 - win-ms09kb974455-update
 - win-ms09kb974571-update
 - win-ms09kb975254-update
 - win-ms09kb975467-update
 - win-ms09kb975682-update
 - win-no-dotnet-security-updates
 - win-no-security-updates
- o Updated Checks
 - win-ms06kb917283-update
 - win-ms06kb917953-update
 - win-ms06kb922770-update
 - win-ms07kb926122-update
 - win-ms07kb931212-update
 - win-ms07kb931768-update
 - win-ms07kb933566-update
 - win-ms07kb935966-update
 - win-ms07kb937143-update
 - win-ms07kb939653-update
 - win-ms07kb941672-update
 - win-ms07kb942615-update
 - win-ms08kb941644-update
 - win-ms08kb944533-update
 - win-ms08kb946538-update
 - win-ms08kb947864-update
 - win-ms08kb948745-update
 - win-ms08kb950759-update
 - win-ms08kb953230-update
 - win-ms08kb953235-update
 - win-ms08kb953838-update

Title: Assuria Auditor AutoUpdate #100 released
Number: 104 **Date:** 31 October 2009

- win-ms08kb956390-update
- win-ms08kb957280-update
- win-ms09kb957638-update
- win-ms08kb958215-update
- win-ms08kb960714-update
- win-ms08kb961371-update
- win-ms09kb962238-update
- win-ms09kb963027-update
- win-ms09kb969897-update

o Updated Policies

- Initial-1
- Initial-5
- Initial-All
- Maintenance-1
- Maintenance-3
- Maintenance-All
- sys-info
- VersionChecks

o Auto Update Files

- rulesets/unarchivePolicy
- signatures/rulesets/unarchivePolicy.sgn
- lib/xpud3_100.zip
- lib/xpud3_100.sgn
- etc/update.ini

**Microsoft Windows
Server 2008**

o Updated Files

- bin/procs/tools.tcl

o New Checks

- load-user-vguids
- reg-autorun-03
- reg-autorun-04
- usb-report
- win-ms09kb957488-update
- win-ms09kb971486-update
- win-ms09kb973525-update
- win-ms09kb973965-update
- win-ms09kb974378-update
- win-ms09kb974455-update
- win-ms09kb974571-update
- win-ms09kb975254-update
- win-ms09kb975467-update
- win-ms09kb975517-update
- win-ms09kb975682-update
- win-no-dotnet-security-updates

Title: Assuria Auditor AutoUpdate #100 released

Number: 104

Date: 31 October 2009

- o Updated Checks
 - win-ms08kb947864-update
 - win-ms08kb950759-update
 - win-ms08kb953230-update
 - win-ms08kb953235-update
 - win-ms08kb953838-update
 - win-ms08kb956390-update
 - win-ms08kb958215-update
 - win-ms08kb960714-update
 - win-ms08kb961371-update
 - win-ms09kb962238-update
 - win-ms09kb963027-update
 - win-ms09kb969897-update

- o Updated Policies
 - Initial-1
 - Initial-5
 - Initial-All
 - Maintenance-1
 - Maintenance-3
 - Maintenance-All
 - PatchChecks

- o Auto Update Files
 - rulesets/unarchivePolicy
 - signatures/rulesets/unarchivePolicy.sgn
 - lib/xpud3_100.zip
 - lib/xpud3_100.sgn
 - etc/update.ini

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

- o Updated Policies
 - Initial-1
 - Initial-5
 - Initial-All
 - Maintenance-1
 - Maintenance-3
 - Maintenance-All
 - PatchChecks

- o New Checks
 - load-user-vguids
 - reg-autorun-03
 - reg-autorun-04
 - usb-report
 - win-ms09kb957488-update

**Microsoft Windows
Vista**

Title: Assuria Auditor AutoUpdate #100 released

Number: 104

Date: 31 October 2009

- win-ms09kb971486-update
- win-ms09kb973525-update
- win-ms09kb973965-update
- win-ms09kb974378-update
- win-ms09kb974455-update
- win-ms09kb974571-update
- win-ms09kb975254-update
- win-ms09kb975467-update
- win-ms09kb975517-update
- win-ms09kb975682-update
- win-no-dotnet-security-updates

o Updated Checks

- win-ms08kb947864-update
- win-ms08kb950759-update
- win-ms08kb953235-update
- win-ms08kb953838-update
- win-ms08kb956390-update
- win-ms08kb958215-update
- win-ms08kb960714-update
- win-ms08kb961371-update
- win-ms09kb963027-update
- win-ms09kb969897-update

o Auto Update Files

- rulesets/unarchivePolicy
- signatures/rulesets/unarchivePolicy.sgn
- lib/xpud3_100.zip
- lib/xpud3_100.sgn
- etc/update.ini

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

o New Checks

- oo-securetty-console
- tdfc-user-profile-exist

o Updated Checks

- SuSE-SA-2006-045
- SuSE-SA-2006-051
- SuSE-SA-2006-058
- SuSE-SA-2006-062
- SuSE-SA-2006-067
- SuSE-SA-2007-014
- SuSE-SA-2007-016
- SuSE-SA-2007-051
- SuSE-SA-2009-021
- SuSE-SA-2009-036
- SuSE-SA-2009-039
- SuSE-SA-2009-042

Title: Assuria Auditor AutoUpdate #100 released

Number: 104

Date: 31 October 2009

- SuSE-SA-2009-045

- o Updated policies

- Initial-1
- Initial-All
- Maintenance-1
- Maintenance-All
- ssa
- sys-cfgs

- o Auto Update Files

- rulesets/unarchivePolicy
- signatures/rulesets/unarchivePolicy.sgn
- lib/xpud3_100.zip
- lib/xpud3_100.sgn
- etc/update.ini

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

- o New Checks

- oo-securetty-console
- tdfc-user-profile-exist

- o Updated Checks

- SuSE-SA-2006-045
- SuSE-SA-2006-051
- SuSE-SA-2006-058
- SuSE-SA-2006-062
- SuSE-SA-2006-067
- SuSE-SA-2007-014
- SuSE-SA-2007-016
- SuSE-SA-2007-051
- SuSE-SA-2009-021
- SuSE-SA-2009-036
- SuSE-SA-2009-039
- SuSE-SA-2009-042
- SuSE-SA-2009-045

- o Updated policies

- Initial-1
- Initial-All
- Maintenance-1
- Maintenance-All
- ssa
- sys-cfgs

- o Auto Update Files

- rulesets/unarchivePolicy
- signatures/rulesets/unarchivePolicy.sgn
- lib/xpud3_100.zip

Title: Assuria Auditor AutoUpdate #100 released

Number: 104

Date: 31 October 2009

- lib/xpud3_100.sgn
- etc/update.ini

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

- o New Checks
 - oo-securetty-console
 - RHSA-2009-1426
 - RHSA-2009-1427
 - RHSA-2009-1428
 - RHSA-2009-1430
 - RHSA-2009-1431
 - RHSA-2009-1432
 - RHSA-2009-1438
 - RHSA-2009-1451
 - RHSA-2009-1452
 - RHSA-2009-1453
 - RHSA-2009-1455
 - RHSA-2009-1457
 - RHSA-2009-1459
 - RHSA-2009-1463
 - RHSA-2009-1465
 - RHSA-2009-1466
 - RHSA-2009-1469
 - RHSA-2009-1470
 - RHSA-2009-1471
 - RHSA-2009-1472
 - RHSA-2009-1484
 - RHSA-2009-1485
 - RHSA-2009-1490
 - tdfc-user-profile-exist
- o Updated Checks
 - RHSA-2005-751
 - RHSA-2005-767
 - RHSA-2005-793
 - RHSA-2005-802
 - RHSA-2005-803
 - RHSA-2006-0658
 - RHSA-2006-0674
 - RHSA-2006-0675
 - RHSA-2006-0676
 - RHSA-2006-0677
 - RHSA-2006-0689
 - RHSA-2006-0695
 - RHSA-2007-0913
 - RHSA-2007-0936
 - RHSA-2007-0937
 - RHSA-2007-0938
 - RHSA-2007-0951

Title: Assuria Auditor AutoUpdate #100 released

Number: 104

Date: 31 October 2009

- RHSA-2009-1106
- RHSA-2009-1148
- RHSA-2009-1162
- RHSA-2009-1184
- RHSA-2009-1186
- RHSA-2009-1188
- RHSA-2009-1189
- RHSA-2009-1190
- RHSA-2009-1193
- RHSA-2009-1364

o Updated Policies

- Initial-1
- Initial-All
- Maintenance-1
- Maintenance-All
- rlsa
- sys-cfgs

o Auto Update Files

- rulesets/unarchivePolicy
- signatures/rulesets/unarchivePolicy.sgn
- lib/xpud3_99.zip
- lib/xpud3_99.sgn
- etc/update.ini

Sun Solaris 8

o Updated Patch Databases

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

o Auto Update Files

- rulesets/unarchivePolicy
- signatures/rulesets/unarchivePolicy.sgn
- lib/xpud3_100.zip
- lib/xpud3_100.sgn
- etc/update.ini

Sun Solaris 9

o New Checks

- oo-basic-security
- tdfc-md5
- tdfc-user-profile-exist

o Updated Policies

- Initial-1
- Initial-All
- Maintenance-1
- Maintenance-All

Title: Assuria Auditor AutoUpdate #100 released
Number: 104 Date: 31 October 2009

- sys-cfgs
- o Updated Patch Databases
 - bin/patch_Solaris.data
 - bin/patch_Solaris.ref
- o Auto Update Files
 - rulesets/unarchivePolicy
 - signatures/rulesets/unarchivePolicy.sgn
 - lib/xpud3_100.zip
 - lib/xpud3_100.sgn
 - etc/update.ini

Sun Solaris 10 (SPARC)

- o New Checks
 - oo-basic-security
 - tdfc-md5
 - tdfc-user-profile-exist
- o Updated Policies
 - Initial-1
 - Initial-All
 - Maintenance-1
 - Maintenance-All
 - sys-cfgs
- o Updated Checks
 - sendmail-daemon-enabled
- o Updated Patch Databases
 - bin/patch_Solaris.data
 - bin/patch_Solaris.ref
- o Auto Update Files
 - rulesets/unarchivePolicy
 - signatures/rulesets/unarchivePolicy.sgn
 - lib/xpud3_100.zip
 - lib/xpud3_100.sgn
 - etc/update.ini

VMware ESX 3.5

No changes this month