Sonntag, 23. September 2007

SMS 2003 Offline Inventory Tool

Summary

SMMHWInv.exe is a tool to get SMS (Microsoft System Management Server) Inventory data from Systems without an SMS Agent or Systems which do not have a network connection.

Project Homepage: http://sourceforge.net/projects/smshwinv

Donations: http://sourceforge.net/donate/index.php?group_id=205237

License

SMSHWInv (SMS2003 Offline Inventory Tool)
Copyright © 2007 by Roger Zander

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 3 of the License, or (at your option) any later version.

 This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

Requirements and prerequisites

The Tool is tested on the following Operating Systems:

- Windows XP
- Windows Server 2003
- Windows Vista

SMSHWInv.exe is a .NET application which requires the Microsoft .NET Framework 2.0.

The following Files are required to run the Tool:

- SMSHWInv.exe
- SMS_Def.mof
  (Defines the SMS reporting Schema. This File can be replaced with the SMS_Def.mof on your SMS Server)

Recommendation

It's recommended to have an actual Version of SMS Agent installed even if the System does not have a network connection. During the Installation of the SMS2003 Agent, additional WMI Providers will be installed which are required for some new reporting features (like in SMS2003 SP3). The SMS Agent Service can be disabled or unassigned from an SMS Site.

Security Impact

This Tool demonstrate how easy the Inventory of a System can be faked, or the SMS Database can be flooded or modified.

Sonntag, 23. September 2007

Disabling IDMIF Inventory as a Agent Setting does not prevent the Server to import IDMIF Files at all. An Attacker is still able to upload DDR and IDMIF Files to an SMS Client Access Point (CAP) . It's strongly recommended to modify the permission on SMS Client Access Point to prevent normal users of uploading DDR and IDMIF Files.

Usage

SMSHWInv.exe <Path to store IDMIF and DDR File>

Or check out the example: getinv.cmd

Upload captured Inventory Files to an SMS Server (CAP)

1. Update DataDiscoveryRecord (DDR)

To make a System available within SMS, a DDR must be generated and uploaded to the SMS Server.

SMSHWInv will generate a DDR-File in the Subfolder DDR of your specified path. Copy this File(s) and paste it to: \\<SMSServer>\CAP_<SMS SiteCode>\ ddr.box.

Wait a couple of minutes and verify if the Systems are visible in the "All Systems" Collection (don't forget to refresh the Collection !).

2. Upload the IDMIF file(s)

Upload the captured IDMIF files to: "\\<SMSServer>\CAP_<SMS Site Code>\Inventry.box" .

Verify the datalrd.log file on the SMS Server if the IDMIF Files are successfully parsed into SMS.

Open the Resource Explorer of the Client and verify if the Hardware Inventory is visible.

Known Issues

- The SMS_Def.mof of SMS2003SP3 has some WMI Classes which are only available if an SMS Agent is installed .