Office 2010 and Office 2013 Benchmark Use

There is a unique challenge with benchmarks for products such as Microsoft Office because of the user context under which the check is conducted. The Microsoft Office Benchmarks make use of many checks against the HKEY\_CURRENT\_USER registry hive. Within DoD, two of our primary SCAP tools are the SCC tool and HBSS Policy Auditor. The SCC tool provides special handling beyond the OVAL specification in this case, checking the user-specific registry databases that exist on the system under test. In the case of the HBSS Policy Auditor tool, it will check for the hive associated with the user context that is running the scan. When run via ePO, PA is run in the context of a system user that does not have these application configurations, leading to false results. The most recent version of OVAL (5.11) includes a new capability which generally follows the SCC tool approach, which will allow for a tool-agnostic way of performing these checks when the SCAP specification, tools, and content are updated to this version. We don't prohibit anyone from running the benchmarks in any application other than SCC, but we can't be assured that the benchmarks will execute correctly.

Only the settings for actual users need to be validated (i.e., those which can interactively login and actually use Microsoft Office).

A way to validate all users who have ever logged onto a box is to check the HKEY\_Users\SID\Software\Policies\Microsoft\office\15.0\.... hive for each profile on the system.

In such case, even the manual STIG could result in false positives if a user hasn't logged in to receive group policy in a while. His hive would only have the settings as they were when he last logged in, which may or may not be compliant.

From a manual STIG standpoint, short of changing verbiage in all three Office STIGs directing reviewers to validate the HKEY\_Users hive for every profile on the workstation, we will be updating the Office Overview documents to state that all users must get the Group Policy, that the reviewer should, at a minimum, validate the profile/registry of the account under which he is logged in, but ideally check HKEY\_Users for all profiles.

NOTE: SCC scanning of ALL user profiles, some notes may be needed for awareness:

-- The SCC scanner will check ALL user profiles for the Office "HKCU" benchmark settings.

-- If even one profile does not meet an Audit, it will be scored as a failure. For example, if 50 each domain user profiles are good but a single local user profile is bad, it is marked as failed.

-- Local user accounts only receive local policy and will never benefit from Domain GPOs. It is therefore highly recommended to apply STIG settings in both local policy and domain policy (when domain-joined) so that both local and domain account profiles will meet STIG benchmarks.

-- STIG settings that are applied as HKCU/User settings must be in place before/during a logon session to get applied to the user profile and in-turn pass a benchmark scan. For example, a local user account that is created before local policy is configured will need to logon to become "compliant".

-- User accounts that don't have a user profile will fail a benchmark scan too. These can occur from certain migration or other account maintenance actions.