the CENTER for INTERNET SECURITY

Security Configuration Benchmark For

Microsoft Office 2007

Version 1.0.0

December 18th, 2009

http://cisecurity.org

feedback@cisecurity.org

Background.

CIS provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and other services and materials from the CIS website or elsewhere ("**Products**") as a public service to Internet users worldwide. Recommendations contained in the Products ("**Recommendations**") result from a consensus-building process that involves many security experts and are generally generic in nature. The Recommendations are intended to provide helpful information to organizations attempting to evaluate or improve the security of their networks, systems and devices. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a "quick fix" for anyone's information security needs.

No representations, warranties and covenants.

CIS makes no representations, warranties or covenants whatsoever as to (i) the positive or negative effect of the Products or the Recommendations on the operation or the security of any particular network, computer system, network device, software, hardware, or any component of any of the foregoing or (ii) the accuracy, reliability, timeliness or completeness of any Product or Recommendation. CIS is providing the Products and the Recommendations "as is" and "as available" without representations, warranties or covenants of any kind.

User agreements.

By using the Products and/or the Recommendations, I and/or my organization ("**we**") agree and acknowledge that:

No network, system, device, hardware, software or component can be made fully secure;
We are using the Products and the Recommendations solely at our own risk;

We are not compensating CIS to assume any liabilities associated with our use of the Products or the Recommendations, even risks that result from CIS's negligence or failure to perform;

We have the sole responsibility to evaluate the risks and benefits of the Products and Recommendations to us and to adapt the Products and the Recommendations to our particular circumstances and requirements;

Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades or bug fixes or to notify us if it chooses at it sole option to do so; and

Neither CIS nor any CIS Party has or will have any liability to us whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages (including without limitation loss of profits, loss of sales, loss of or damage to reputation, loss of customers, loss of software, data, information or emails, loss of privacy, loss of use of any computer or other equipment, business interruption, wasted management or other staff resources or claims of any kind against us from third parties) arising out of or in any way connected with our use of or our inability to use any of the Products or Recommendations (even if CIS has been advised of the possibility of such damages), including without limitation any liability associated with infringement of intellectual property, defects, bugs, errors, omissions, viruses, worms, backdoors, Trojan horses or other harmful items.

Grant of limited rights.

CIS hereby grants each user the following rights, but only so long as the user complies with all of the terms of these Agreed Terms of Use:

Except to the extent that we may have received additional authorization pursuant to a written agreement with CIS, each user may download, install and use each of the Products on a single computer;

Each user may print one or more copies of any Product or any component of a Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, provided that all such copies are printed in full and are kept intact, including without limitation the text of this Agreed Terms of Use in its entirety.

Retention of intellectual property rights; limitations on distribution.

The Products are protected by copyright and other intellectual property laws and by international treaties. We acknowledge and agree that we are not acquiring title to any intellectual property rights in the Products and that full title and all ownership rights to the Products will remain the exclusive property of CIS or CIS Parties. CIS reserves all rights not expressly granted to users in the preceding section entitled "Grant of limited rights." Subject to the paragraph entitled "Special Rules" (which includes a waiver, granted to some classes of CIS Members, of certain limitations in this paragraph), and except as we may have otherwise agreed in a written agreement with CIS, we agree that we will not (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code for any software Product that is not already in the form of source code; (ii) distribute, redistribute, encumber, sell, rent, lease, lend, sublicense, or otherwise transfer or exploit rights to any Product or any component of a Product; (iii) post any Product or any component of a Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device, without regard to whether such mechanism or device is internal or external, (iv) remove or alter trademark, logo, copyright or other proprietary notices, legends, symbols or labels in any Product or any component of a Product; (v) remove these Agreed Terms of Use from, or alter these Agreed Terms of Use as they appear in, any Product or any component of a Product; (vi) use any Product or any component of a Product with any derivative works based directly on a Product or any component of a Product; (vii) use any Product or any component of a Product with other products or applications that are directly and specifically dependent on such Product or any component for any part of their functionality, or (viii) represent or claim a particular level of compliance with a CIS Benchmark, scoring tool or other Product. We will not facilitate or otherwise aid other individuals or entities in any of the activities listed in this paragraph.

We hereby agree to indemnify, defend and hold CIS and all of its officers, directors, members, contributors, employees, authors, developers, agents, affiliates, licensors, information and service providers, software suppliers, hardware suppliers, and all other persons who aided CIS in the creation, development or maintenance of the Products or Recommendations ("**CIS Parties**") harmless from and against any and all liability, losses, costs and expenses (including attorneys' fees and court costs) incurred by CIS or any CIS Party in connection with any claim arising out of any violation by us of the preceding paragraph, including without limitation CIS's right, at our expense, to assume the exclusive defense and control of any matter subject to this indemnification, and in such case, we agree to cooperate with CIS in its defense of such claim. We further agree that all CIS Parties are third-party beneficiaries of our undertakings in these Agreed Terms of Use.

Special rules.

CIS has created and will from time to time create special rules for its members and for other persons and organizations with which CIS has a written contractual relationship. Those special rules will override and supersede these Agreed Terms of Use with respect to the users who are covered by the special rules. CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to distribute the Products and Recommendations within such Member's own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that the foregoing grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Choice of law; jurisdiction; venue.

We acknowledge and agree that these Agreed Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland, that any action at law or in equity arising out of or relating to these Agreed Terms of Use shall be filed only in the courts located in the State of Maryland, that we hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action. If any of these Agreed Terms of Use shall be determined to be unlawful, void, or for any reason unenforceable, then such terms shall be deemed severable and shall not affect the validity and enforceability of any remaining provisions. We acknowledge and agree that we have read these Agreed Terms of Use in their entirety, understand them and agree to be bound by them in all respects.

Table of Contents

Overview

This document, *Security Configuration Benchmark for Microsoft Office 2007*, provides prescriptive guidance for establishing a secure configuration posture for Microsoft Office version 2007 running on Windows XP and Windows Vista. This guide was tested against Microsoft Office 2007 Ultimate. To obtain the latest version of this guide, please visit http://cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Consensus Guidance

This guide was created using a consensus review process comprised of volunteer and contract subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been released to the public Internet. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the CIS benchmark. If you are interested in participating in the consensus review process, please send us a note to feedback@cisecurity.org.

Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Microsoft Office 2007 on a Microsoft Windows platform.

Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Authors
Shyama Rose, *Leviathan Security Group*
Stephanie Smith, *Leviathan Security Group*

Typographic Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples.

	Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Configuration Levels

This section defines the configuration levels that are associated with each benchmark recommendation. Configuration levels represent increasing levels of security assurance.

Level-I Benchmark settings/actions

Level-I Benchmark recommendations are intended to:

- be practical and prudent;
- provide a clear security benefit; and
- do not negatively inhibit the utility of the technology beyond acceptable means

Level-II Benchmark settings/actions

Level-II Benchmark recommendations exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is paramount
- acts as defense in depth measure
- may negatively inhibit the utility or performance of the technology

Scoring Status

This section defines the scoring statuses used within this document. The scoring status indicates whether compliance with the given recommendation is discernable in an automated manner.

Scorable

The platform's compliance with the given recommendation can be determined via automated means.

Not Scorable

The platform's compliance with the given recommendation cannot be determined via automated means.

Explanation of this Document

This document is a general guide for using Group Policy to secure Microsoft Office 2003 SP3 & 2007 installed on Microsoft Windows XP and Windows Server 2003. This document makes wide use of the Office Group Policy templates available in the respective Microsoft Office Resource Kits, and closely follows the Microsoft's security recommendations as

found in the 2007 Microsoft Office Security Guide. The relevant Resource Kit should be installed before using this document.

The listings within this document are formatted in the following manner:

Description
DESCRIPTION OF THE GPO

Rationale
RATIONALE REGARDING THE RECOMMENDED STATE FOR THIS GPO

Settings: GROUP POLICY PATH TO THE GPO				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
NAME OF THE GPO	STATE One of: Enabled, Disabled, Not Configured	2003 Or 2007	I Or II	S Or N

Audit
INSTRUCTIONS ON HOW TO DETERMINE WHETHER THE GPO IS SET AS SUGGESTED

Remediation
INSTRUCTIONS ON HOW TO SET THE GPO AS SUGGESTED

Additional References
OPTIONAL OUTSIDE REFERENCE, APPLICABLE TO THE GPO

Information regarding definitions of **Level** and **Scorability** can be found below. It should be noted that some recommended states are multi-part. Most commonly they require the selection of additional configuration options from a drop-down list box in the Group Policy tool when Enabled. When this is the case, the additional setting will be listed in the **Recommended State** cell, on a line below the initial state.

Unless otherwise noted, the **Setting** path is relative to:

```
Local Computer Policy\User Configuration\Administrative Templates
```

General Guidance

This benchmark consists of Microsoft Group Policy recommendations. Group Policy is an infrastructure in Microsoft Windows that allows an administrator to implement specific application configurations for Users and computers in a network. The policy settings, contained in Group Policy Objects (GPOs), can be loaded onto an operating system by installing policy templates (.adm files) for various applications. There are two main benefits of configuring Group Policies over other mechanisms: Group policies are reapplied regularly (either at login or at a specified time interval) and are not modifiable by Users.

Group Policies are flexible in that they can be configured for specific Users or for the entire system.

The *Microsoft Office 2007 Resource Kit* contains a substantive collection of Group Policy templates for Office 2007. More information, including Instructions for downloading and installing the Office 2007 policy templates can be found here: *http://support.microsoft.com/kb/924617*.

1. Recommendations

1.1. System

1.1.1. System Configuration

All **Settings** paths in this section are relative to:

Local Computer Policy\Computer Configuration\Administrative Settings

1.1.1.1. Office Updates: Level I

Description
The **Block updates from the Office Update Site from applying** option determines if a User may acquire updates from the Microsoft Office Update site, the Check for Updates menu and task pane items.

Rationale
Setting this option to **Disabled** allows Users to apply newly released updates as soon as they become available reduces risk by eliminating security flaws addressed by the updates. **Note:** For systems that are enrolled in a centralized patch management solution, administrators should consider disabling automatic updates by setting this option to **Enabled**.

Settings: ..\Microsoft Office 2007 system\Miscellaneous				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Block updates from the Office Update Site from applying	Disabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\Common\OfficeUpdate 3. Ensure that the BlockUpdates DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK.

2. Locate and select:
   User Configuration\Administrative Templates\
      Microsoft Office 2007 system\Miscellaneous
3. Double-Click Block updates from the Office Update Site from applying.
4. Select Disabled, click OK.

Additional References
CCE-784-9

1.1.1.2. Office Updates: Level II

Description
The **Block updates from the Office Update Site from applying** option determines if a User may acquire updates from the Microsoft Office Update site, the Check for Updates menu and task pane items.

Rationale
Applying updates without testing may result in reduced availability of applications installed on core enterprise infrastructure and lead to divergent configuration schemes on various machines. Many enterprise level environments have patch management teams and mechanisms such as IPS that helps mitigate the risk of un-updated enterprise systems for the short interim of testing before updates are rolled out.

Settings: ..\Microsoft Office 2007 system\Miscellaneous				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Block updates from the Office Update Site from applying	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\Common\OfficeUpdate 3. Ensure that the BlockUpdates DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Miscellaneous 3. Double-Click Block updates from the Office Update Site from applying. 4. Select Enabled, click OK.

Additional References

CCE-784-9

1.1.1.3. Disable Repairing Corrupt Office Open XML: Level II

Description
By default, an Office application will prompt the User with the option of repairing a corrupt Office Open XML if corruption is detected.

Rationale
Setting this option to **Enabled** reduces the attack surface area of the Office application suite by denying the User prompting due to file corruption.

Settings: ...\Microsoft Office 2007 system (Machine)\Security Settings				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable Package Repair	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Office\12.0\Common\ OpenXMLFormat 3. Ensure that the DisablePackageRepair DWORD exists and is set to 1

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: Computer Configuration\Administrative Templates\ Microsoft Office 2007 system (machine)\Security Settings 3. Double-Click Disable Package Repair. 4. Select Enabled, click OK.

Additional References
CCE-933-2

1.1.1.4. Prevent Using Visual Basic for Applications: Level II

Description
The **Disable VBA for Office applications** setting will prevent Excel, FrontPage, Outlook, PowerPoint, Publisher and Word from using Visual Basic for Applications (VBA), despite whether or not the VBA feature is installed. Changing this setting will not install or remove the VBA files from the machine.

Rationale
Disabling this option reduces the attack surface area of the Office system.

Settings: ...\Microsoft Office 2007 system (Machine)\Security Settings				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable VBA for Office applications	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Office\12.0\Common 3. Ensure that the VbOff DWORD exists and is set to 1

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: Computer Configuration\Administrative Templates\ Microsoft Office 2007 system (machine)\Security Settings 3. Double-Click Disable VBA for Office applications. 4. Select Enabled, click OK.

Additional References
CCE-116-4

1.1.1.5. URL Syntax That Includes Username and Password: Level I

Description
Instances of Internet Explorer within Office applications may be configured to adhere to Internet Explorer's default behavior of invalidating URL syntax that may include a Username and password, such as http://Username:password@server/.

Rationale
This URL form can be abused to deceive users into accessing malicious resources that appear to be legitimate or benign.

Settings: ...\Microsoft Office 2007 system (Machine)\Security Settings\IE Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable User name and password	Enabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK.

2. Locate and select:
   HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Main
   FeatureControl\FEATURE_HTTP_USERNAME_PASSWORD_DISABLE
3. Ensure that the following DWORDs exist and are set to 1:
   groove.exe
   excel.exe
   powerpnt.exe
   pptview.exe
   visio.exe
   outlook.exe
   spDesign.exe
   msaccess.exe
   onent.exe
   winword.exe

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: Computer Configuration\Administrative Templates\ Microsoft Office 2007 system (machine)\Security Settings\IE Security 3. Double-Click Disable User name and password. 4. Select Enabled. 5. Check each of: groove.exe excel.exe powerpnt.exe pptview.exe visio.exe outlook.exe spDesign.exe msaccess.exe onent.exe winword.exe 6. Click OK.

Additional References
CCE-1563-6, CCE-1215-3, CCE-1484-5, CCE-1629-5, CCE-1762-4, CCE-1660-0, CCE-1057-9, CCE-1285-6

1.1.1.6. Internet Explorer's ActiveX Behavior for Office: Level I

Description
Instances of Internet Explorer within Office applications may be configured to adhere to Internet Explorer's default behavior for ActiveX control instantiation, including IE's blacklisting and zone settings.

Rationale
Enabling the **Bind to object** setting allows for stringent restrictions on ActiveX controls by denying instantiation if the kill bit is set in the registry or if the security settings for the control's zone do not allow initialization.

Settings: ...\Microsoft Office 2007 system (Machine)\Security Settings\IE Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Bind to object	Enabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Main FeatureControl\FEATURE_SAFE_BINDTOOBJECT 3. Ensure that the following DWORDs exist and are set to 1: groove.exe excel.exe powerpnt.exe pptview.exe visio.exe outlook.exe spDesign.exe msaccess.exe onent.exe winword.exe

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: Computer Configuration\Administrative Templates\ Microsoft Office 2007 system (machine)\Security Settings\IE Security 3. Double-Click Bind to object. 4. Select Enabled. 5. Check each of: groove.exe excel.exe powerpnt.exe pptview.exe visio.exe outlook.exe spDesign.exe msaccess.exe onent.exe

winword.exe
6. Click OK.

Additional References
CCE-1669-1, CCE-1691-5, CCE-1338-3, CCE-1717-8, CCE-1488-6, CCE-1638-6, CCE-1647-7, CCE-1294-8

1.1.1.7. Internet Explorer within Office to Use a Local Zone: Level I

Description
Instances of Internet Explorer within an Office application may be configured to render Internet-born documents now residing on a UNC path with a more stringent security policy.

Rationale
Files saved from the Internet may contain executable code. Running this code within the lax Local Intranet security zone may give access to resources it otherwise would not be able to access.

Settings: ...\Microsoft Office 2007 system (Machine)\Security Settings\IE Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Saved from URL	Enabled	2007	I	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Internet Explorer\Main FeatureControl\FEATURE_UNC_SAVEDFILECHECK
3. Ensure that the following DWORDs exist and are set to 1:
   groove.exe
   excel.exe
   powerpnt.exe
   pptview.exe
   visio.exe
   outlook.exe
   spDesign.exe
   msaccess.exe
   onent.exe
   winword.exe

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   Computer Configuration\Administrative Templates\

Microsoft Office 2007 system (machine)\Security Settings\IE Security

3. Double-Click Saved from URL.
4. Select Enabled.
5. Check each of:
   groove.exe
   excel.exe
   powerpnt.exe
   pptview.exe
   visio.exe
   outlook.exe
   spDesign.exe
   msaccess.exe
   onent.exe
   winword.exe
6. Click OK.

Additional References
CCE-1193-2, CCE-1352-4, CCE-928-2, CCE-1576-8, CCE-1100-7, CCE-1232-8, CCE-1774-9, CCE-906-8, CCE-1647-7

1.1.2. ActiveX Control Security

1.1.2.1. Initialization of UFI ActiveX Controls: Level I

Description
The **ActiveX Control Initialization** option configures the behavior of Office applications when encountering UFI ActiveX Controls.

Rationale
Enabling this option and setting it to level 2 allows the initialization of UFI ActiveX without warning the User using safe-mode. Safe-mode allows an ActiveX Control to run, but not modify or write data, allowing high usability while restricting the damage of a malicious ActiveX control.

Settings: ..\Microsoft Office 2007 system\Security Settings				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
ActiveX Control Initialization	Enabled 2	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\Security 3. Ensure that the UFIControls DWORD exists and is set to 2.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Security Settings 3. Double-Click ActiveX Control Initialization. 4. Select Enabled, select 2, and click OK.

Additional References
CCE-908-4

1.1.2.2. Initialization of UFI ActiveX Controls: Level II

Description
The **ActiveX Control Initialization** option configures the behavior of Office applications when encountering UFI ActiveX Controls.

Rationale
When disabled, ActiveX Controls marked as UFI will not initialize, reducing attack surface. Disabling this setting may cause usability issues.

Settings: ..\Microsoft Office 2007 system\Security Settings				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
ActiveX Control Initialization	Disabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\Security 3. Ensure that the UFIControls DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Security Settings 3. Double-Click ActiveX Control Initialization. 4. Select Disabled, click OK.

Additional References
CCE-908-4

1.1.2.3. ActiveX Initialization: Level II

Description
The **Disable All ActiveX** setting determines whether ActiveX controls are initialized.

Rationale
Since ActiveX controls have full access to the host machine's file system, untrusted ActiveX controls should be prevented from running. Setting the state as **Enabled** will not initialize ActiveX controls from non-trusted locations. This setting does not notify the User that the ActiveX controls have been disabled.

Settings: ..\Microsoft Office 2007 system\Security Settings				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable All ActiveX	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\Common\Security 3. Ensure that the DisableAllActiveX DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Security Settings 3. Double-Click Disable All ActiveX. 4. Select Enabled, click OK.

Additional References
CCE-1242-7

1.1.3. Office Online Security

1.1.3.1. Internet Faxing: Level II

Description
The **Disable Internet Fax feature** option configures whether to allow Internet Faxing from Office applications.

Rationale
Setting the state of this option to **Enabled** reduces the attack surface area of the Office system by disabling internet faxing from Office applications.

Settings: ..\Microsoft Office 2007 system\Services\Fax				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable Internet Fax feature	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\Services\Fax 3. Ensure that the NoFax DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Services\Fax 3. Double-Click Disable Internet Fax feature. 4. Select Enabled, click OK.

Additional References
CCE-1061-1

1.1.3.2. Restrict All Content from Microsoft Office Online: Level II

Description
The **Online content options** option allows for the configuration of online content in all Office applications.

Rationale
Configuring this option to **Never show online content or entry points** reduces the attack surface area of the Office system by restricting all content and links from Microsoft Office Online

Settings: ..\Microsoft Office 2007 system\Tools | Options | General | Service Options...\Online Content				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Online content options	Enabled Never show online content or entry points	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select:

HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\Internet
3. Ensure that the UseOnlineContent DWORD exists and is set to 0.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
   Microsoft Office 2007 system\Tools | Options | General | Service Options...\Online Content
3. Double-Click Online content options.
4. Select Enabled, select Never show online content or entry points, and click OK.

Additional References

CCE-967-0

1.1.3.3. Require Users to Connect to Verify Permission: Level I

Description

When opening an Office document with Information Rights Management (IRM) permissions, setting this option forces a User to connect to the Internet or local area network to confirm their license by Windows Live ID or Rights Management Services (RMS).

Rationale

Setting this option to **Enabled** prevents Users from potentially bypassing IRM if the access is cached.

Settings: ..\Microsoft Office 2007 system\Manage Restricted Permissions

Group Policy Object	Recommended State	Version	Level	Scorability
Always require Users to connect to verify permission	Enabled	2007	I	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\DRM
3. Ensure that the requireConnection DWORD exists and is set to 1.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
   Microsoft Office 2007 system\Manage Restricted Permissions
3. Double-Click Always require Users to connect to verify permission.

4. Select Enabled, click OK.

Additional References
CCE-1493-6

1.1.3.4. Download of ClipArt: Level II

Description
The **Disable Clip Art and Media downloads from the client and from Office Online website** option determines whether a User is allowed to download Clip Art and Media from either the Clip Art pane or Office Online.

Rationale
Enabling this option reduces the attack surface area of the Office system by disabling the ability to download content from the Office Online website.

Settings: ..\Microsoft Office 2007 system\Tools | Options | General | Web Options...				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable Clip Art and Media downloads from the client and from Office Online website	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\Internet 3. Ensure that the DisableClipArtAndMediaDownload DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Options | General | Web Options... 3. Double-Click Disable Clip Art and Media downloads from the client and from Office Online website. 4. Select Enabled, click OK.

Additional References
CCE-1458-9

1.1.3.5. Download of Templates: Level II

Description
The **Disable template downloads from the client and from Office Online website** option

determines whether a User can download Templates from Office Online.

Rationale
Setting this option to **Enabled** prevents downloading of Templates from Office Online which may contain malicious macros or ActiveX controls that can harm a User's computer.

Settings: ..\Microsoft Office 2007 system\Tools | Options | General | Web Options...				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable template downloads from the client and from Office Online website	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\Internet 3. Ensure that the DisableTemplateDownload DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Options | General | Web Options... 3. Double-Click Disable template downloads from the client and from Office Online website. 4. Select Enabled, click OK.

Additional References
CCE-1233-6

1.1.3.6. Download of Add-Ins and Patches: Level II

Description
The **Disable access to updates, add-ins, and patches on the Office Online website** option determines whether a User may access the Office Online website for updates, add-ins, and patches.

Rationale
Setting this option to **Enabled** prevents downloading of add-ins from Office Online which may contain malicious code that can harm a User's computer.

Settings: ..\Microsoft Office 2007 system\Tools | Options | General | Web Options...				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**

Disable access to updates, add-ins, and patches on the Office Online website	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\Internet 3. Ensure that the DisableDownloadCenterAccess DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Options | General | Web Options... 3. Double-Click Disable access to updates add-ins and patches on the Office Online website. 4. Select Enabled, click OK.

Additional References
CCE-1379-7

1.1.3.7. Download of Training Practice Files: Level II

Description
The **Disable training practice downloads from the Office Online website** option determines whether a User can download training practice files from the Office Online website.

Rationale
Setting this option to **Enabled** prevents the download of training practice files from Office Online. These template files may possibly contain malicious macros or ActiveX controls which can harm a User's computer.

Settings: ..\Microsoft Office 2007 system\Tools | Options | General | Web Options...				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable training practice downloads from the Office Online website	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\Internet 3. Ensure that the DisableTrainingPracticeDownload DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Options | General | Web Options... 3. Double-Click Disable training practice downloads from the Office Online website. 4. Select Enabled, click OK.

Additional References
CCE-1528-9

1.1.3.8. Templates Upload: Level II

Description
The **Prevents Users from uploading document templates to the Office Online community** option determines whether a User can upload templates Office Online website.

Rationale
Enabling this option prevents the inadvertent leak of hidden, sensitive data by Users uploading templates to Office Online.

Settings: ..\Microsoft Office 2007 system\Tools | Options | General | Web Options...				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Prevents Users from uploading document templates to the Office Online community	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\Internet 3. Ensure that the DisableCustomerSubmittedUpload DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Options | General | Web Options... 3. Double-Click Prevents Users from uploading document templates to the Office Online community.. 4. Select Enabled, click OK.

Additional References

CCE-1401-9

1.1.3.9. Customer-Submitted Templates: Level I

Description
The **Disable customer-submitted templates downloads from Office Online** option determines whether a User can download customer-submitted templates from the Office Online website.

Rationale
Enabling this option prevents Templates from being downloaded from Office Online, which may contain malicious macros or ActiveX controls that could harm a User's computer.

Settings: ..\Microsoft Office 2007 system\Tools | Options | General | Web Options...				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable customer-submitted templates downloads from Office Online	Enabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\Internet 3. Ensure that the DisableCustomerSubmittedDownload DWORD does not exist.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Options | General | Web Options... 3. Double-Click Disable a customer-submitted template downloads from Office Online. 4. Select Not Configured, click OK.

Additional References
CCE-1533-9

1.1.3.10. Retrieving Links: Level II

Description
The **Disable the Office client from polling the Office server for published links** option determines if Office applications can retrieve lists of published links for the opening and saving of files from SharePoint Server sites.

Rationale
If a list of published links is accessible, a malicious Use may publish malicious links which

may inadvertently leak sensitive data.

Settings: ..\Microsoft Office 2007 system\Server Settings				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable the Office client from polling the Office server for published links	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\Portal 3. Ensure that the LinkPublishingDisabled DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Server Settings 3. Double-Click Disable the Office client from polling the Office server for published links. 4. Select Enabled, click OK.

Additional References
CCE-1545-3

1.1.4. UI Customization Security

1.1.4.1. Customer Experience Program: Level II

Description
The **Enable Customer Experience Improvement Program** option determines whether Users may participate in Microsoft's Customer Experience Improvement Program.

Rationale
Setting this option to **Disabled** reduces the attack surface area of the Office system.

Settings: ..\Microsoft Office 2007 system\Privacy\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Enable Customer Experience Improvement Program	Disabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK.

2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common
3. Ensure that the QMEnable DWORD exists and is set to 0.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
      Microsoft Office 2007 system\Privacy\Trust Center
3. Double-Click Enable Customer Experience Improvement Program.
4. Select Disabled, click OK.

Additional References

CCE-184-2

1.1.4.2. Initialization Control in Forms3: Level II

Description

The **Enable Customer Experience Improvement Program** option determines whether Users may participate in Microsoft's Customer Experience Improvement Program.

Rationale

Setting this option to **Enabled** reduces the attack surface area of the Office system by allowing administrators to specific how the control is loaded.

Settings: ..\Microsoft Office 2007 system\Security Settings

Group Policy Object	Recommended State	Version	Level	Scorability
Load Controls in Forms3	Enabled 1	2007	II	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\VBA\Security
3. Ensure that the LoadControlsInForms DWORD exists and is set to 1.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
      Microsoft Office 2007 system\Security Settings
3. Double-Click Load Controls in Forms3.
4. Select Enabled, select 1, and click OK.

Additional References
CCE-1068-6

1.1.4.3. Disable UI Extending from Documents: Level II

Description
When enabled, this option disables Office application documents and templates from extending the application UI.

Rationale
As the functionality of the new UI is often extended through scripting, enabling this option reduces the attack surface area of the Office system.

Settings: ..\Microsoft Office 2007 system\Global Options\Customize				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable UI extending from documents and templates	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\Toolbars 3. Ensure that the NoExtensibilityCustomizationFromDocument DWORD exists and is set to 1 in each of the keys: Access Excel Outlook PowerPoint Word

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Global Options\Customize 3. Double-Click Disable UI extending from documents and templates. 4. Select Enabled 5. Check each of the following: Disallow in Word Disallow in Excel Disallow in PowerPoint Disallow in Access

Disallow in Outlook 6. Click OK.

Additional References
CCE-630-4, CCE-1154-4, CCE-1410-0, CCE-1432-4, CCE-1198-1, CCE-929-0

1.1.4.4. Opt-in Wizard: Level II

Description
The **Disable Opt-in Wizard on first run** option determines whether the Opt-In Wizard is run the first time an Office application is run.

Rationale
Enterprises that have policies restricting the use of external resources should enable this option to prevent the Users to opting-in various Internet-based services.

Settings: ..\Microsoft Office 2007 system\Privacy\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable Opt-in Wizard on first run	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\General 3. Ensure that the ShownOptIn DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Privacy\Trust Center 3. Double-Click Disable Opt-in Wizard on first run. 4. Select Enabled, click OK.

Additional References
CCE-1615-4

1.1.4.5. Suppress External Signature Services: Level II

Description
This option determines whether the **Add Signature Services** menu item is displayed.

Rationale

Enterprises with policies restricting access to external services should enable this option, as it will not allow a User to display a list of signature service providers from the Office Online website.

Settings: ..\Microsoft Office 2007 system\Signing				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Suppress external signature services menu item	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\Signatures 3. Ensure that the SuppressExtSigningSvcs DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Signing 3. Double-Click Suppress external signature services menu item. 4. Select Enabled, click OK.

Additional References
CCE-1220-3

1.1.5. Visual Basic for Applications Security

1.1.5.1. Visual Basic for Applications for Office Applications: Level II

Description
The **Disable VBA for Office applications** setting prevents, regardless of whether or not the Visual Basic for Applications (VBA) feature is installed, Excel, FrontPage, Outlook, PowerPoint, Publisher and Word from using VBA code. Changing this setting will not install or remove the VBA files from the machine.

Rationale
Setting this option to **Enabled** reduces the attack surface area of the Office system.

Settings: ..\Microsoft Office 2007 system\Security Settings				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable VBA for Office applications	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\Security 3. Ensure that the VbaOff DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Security Settings 3. Double-Click Disable VBA for Office applications. 4. Select Enabled, click OK.

Additional References
CCE-116-4

1.1.6. Macro Security

1.1.6.1. Enable/Disable Macros: Level I

Description
The **Automation Security** option dictates whether macros are enabled or disabled within Office applications.

Rationale
Setting this option to **Use application macro security level** allows macro behavior to be determined by individual applications in the Office system.

Settings: ..\Microsoft Office 2007 system\Security Settings				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Automation Security	Enabled Use application macro security level	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\Common\Security 3. Ensure that the AutomationSecurity DWORD exists and is set to 2.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK.

2. Locate and select:
   User Configuration\Administrative Templates\
      Microsoft Office 2007 system\Security Settings
3. Double-Click Automation Security.
4. Select Enabled, select Use application macro security level, and click OK.

Additional References
CCE-1574-3

1.1.6.2. Enable/Disable Macros: Level II

Description
The **Automation Security** option determines whether macros are enabled or disabled within Office applications.

Rationale
Macros pose a potential security threat because they have the capability to execute malicious code. Therefore, setting this option to **Disable macros by default** reduces attack surface area of the application. This setting is global across the Office system.

Settings: ..\Microsoft Office 2007 system\Security Settings				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Automation Security	Enabled Disable macros by default	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\Common\Security 3. Ensure that the AutomationSecurity DWORD exists and is set to 3.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Security Settings 3. Double-Click Automation Security. 4. Select Enabled, select Disable macros by default, and click OK.

Additional References
CCE-1574-3

1.1.7. File Conversion, Opening and Saving Security

1.1.7.1. Opening Prior Versions of Office Documents in Browser: Level II

Description
The **Allow Users with earlier versions of Office to read with browsers** setting will ensure that Office applications always create files that can be read in browsers that support IRM.

Rationale
Setting this option to **Enabled** ensures that IRM and other modern security features cannot be circumvented via a web browser by opening a file in a previous version of Office.

Settings: ..\Microsoft Office 2007 system\Manage Restricted Permissions				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Allow Users with earlier versions of Office to read with browsers	Disabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\DRM 3. Ensure that the IncludeHTML DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Manage Restricted Permissions 3. Double-Click Allow Users with earlier versions of Office to read with browsers.... 4. Select Disabled, click OK.

Additional References
CCE-1612-1

1.1.7.2. Opening Pre-Release File Format Versions (Word): Level I

Description
The **Block opening of pre-release versions of file formats new to Word 2007 through the Compatibility Pack for the 2007 Office system and Word 2007 Open XML/Word 97-2003 Format Converter** option determines whether a User with the Microsoft Office Compatibility Pack for Word File Formats installed can open Office Open XML files saved with pre-release versions of Word 2007.

Rationale

Enabling this option reduces the attack surface area of the Office system.

Settings: ..\Microsoft Office 2007 system\Office 2007 Converters				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Block opening of pre-release versions of file formats new to Word 2007 through the Compatibility Pack for the 2007 Office system and Word 2007 Open XML/Word 97-2003 Format Converter	Enabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Word\Security\FileOpenBlock 3. Ensure that the Word12BetaFilesFromConverters DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Office 2007 Converters 3. Double-Click Block opening of pre-release versions of file formats new to Word 2007 through the Compatibility Pack for the 2007 Office system and Word 2007 Open XML/Word 97-2003 Format Converter. 4. Select Enabled, click OK.

Additional References
CCE-1549-5

1.1.7.3. Block Opening of Malformed URLs: Level I

Description
The **Navigate URL** setting validates URLS and will restrict Users from visiting a malformed URL

Rationale
Malformed URLs may contain requests that could cause security vulnerabilities such as Denial of Service. Setting **Navigate URL** to **Enabled** will prevent vulnerabilities due to badly formed URLs.

Settings: .. Microsoft Office 2007 system (Machine)\Security Settings\IE Security

Group Policy Object	Recommended State	Version	Level	Scorability
Navigate URL	Enabled	2007	I	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_VALIDATE_NAVIGATE_URL
3. Ensure that the following DWORDs exist and are set to 1:
   groove.exe
   excel.exe
   powerpnt.exe
   pptview.exe
   visio.exe
   outlook.exe
   spDesign.exe
   msaccess.exe
   onent.exe
   winword.exe

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   Computer Configuration\Administrative Templates\Microsoft Office 2007 system (Machine)\Security Settings\IE Security
3. Double-Click Navigate URL.
4. Select Enabled.
5. Check each of:
   groove.exe
   excel.exe
   powerpnt.exe
   pptview.exe
   visio.exe
   outlook.exe
   spDesign.exe
   msaccess.exe
   onent.exe
   winword.exe
6. Click OK.

Additional References

CCE-1034, CCE-1435, CCE-1708, CCE-808, CCE-1650, CCE-1223, CCE-176, CCE-1769

1.1.7.4. Block Popups: Level II

Description
The **Block Popups** setting suppresses a majority of unwanted popups that may contain malicious content.

Rationale
Malicious popups can be disruptive or dangerous, posing a security risk. Setting this option to **Enabled** will protect Users' exposure to malicious content by blocking most unwanted popups.

Settings: ..\ Microsoft Office 2007 system (Machine)\Security Settings\IE Security\Block popups				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Block Popups	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_WEBOC_POPUPMANAGEMENT 3. Ensure that the following DWORDs exist and are set to 1: excel.exe powerpnt.exe pptview.exe spDesign.exe outlook.exe msaccess.exe winword.exe

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: Computer Configuration\Administrative Templates\Microsoft Office 2007 system (Machine)\Security Settings\IE Security\Block popups 3. Double-Click Block Popups 4. Select Enabled. 5. Check each of: excel.exe powerpnt.exe pptview.exe spDesign.exe outlook.exe

msaccess.exe
winword.exe
6. Click OK.

Additional References
CCE-1152, CCE-1566, CCE-1077, CCE-1606, CCE-1738, CCE-1262, CCE-1663, CCE-1544

1.1.7.5. Disable Password to Open UI: Level I

Description
If the **Password to Open UI** option is enabled, Users are denied access to the password user interface in all Office applications, disallowing Users to create encrypted files.

Rationale
Users should not be denied Encryption availability because it is an accepted standard method for securing sensitive data and facilitates the mitigation of document threats.

Settings: ..\Microsoft Office 2007 system\Security Settings\				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable password to open UI	Disabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: Software\Policies\Microsoft\Office\12.0\Common\Security 3. Ensure that the DisablePasswordUI DWORD exists and is set to 1:

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: Configuration\Administrative Templates\Microsoft Office 2007 system\Security Settings\ 3. Double-Click Disable password to open UI. 4. Select Disabled, click OK.

Additional References
CCE-1083-5

1.1.7.6. Opening Pre-Release File Format Versions (Excel): Level I

Description
The **Block opening of pre-release versions of file formats new to Excel 2007 through the Compatibility Pack for the 2007 Office system and Excel 2007 Converter** option determines

whether a User with the Microsoft Office Compatibility Pack for Excel File Formats installed can open Office Open XML files saved with pre-release versions of Excel 2007.

Rationale
Enabling this option reduces the attack surface area of the Office system.

Settings: ..\Microsoft Office 2007 system\Office 2007 Converters				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Block opening of pre-release versions of file formats new to Excel 2007 through the Compatibility Pack for the 2007 Office system and Excel 2007 Converter	Enabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Excel\Security\FileOpenBlock 3. Ensure that the Excel12BetaFilesFromConverters DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Office 2007 Converters 3. Double-Click Block opening of pre-release versions of file formats new to Excel 2007 through the Compatibility Pack for the 2007 Office system and Excel 2007 Converter. 4. Select Enabled, click OK.

Additional References
CCE-1431-6

1.1.7.7. Opening Pre-Release File Format Versions (PowerPoint): Level I

Description
The **Block opening of pre-release versions of file formats new to PowerPoint 2007 through the Compatibility Pack for the 2007 Office system and PowerPoint 2007 Converter** option determines whether a User with the Microsoft Office Compatibility Pack for PowerPoint File Formats installed can open Office Open XML files saved with pre-release versions of PowerPoint 2007.

Rationale

Enabling this option reduces the attack surface area of the Office system.

Settings: ..\Microsoft Office 2007 system\Office 2007 Converters				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Block opening of pre-release versions of file formats new to PowerPoint 2007 through the Compatibility Pack for the 2007 Office system and PowerPoint 2007 Converter	Enabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\PowerPoint\Security\FileOpenBlock 3. Ensure that the PowerPoint12BetaFilesFromConverters DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Office 2007 Converters 3. Double-Click Block opening of pre-release versions of file formats new to PowerPoint 2007 through the Compatibility Pack for the 2007 Office system and PowerPoint 2007 Converter. 4. Select Enabled, click OK.

Additional References
CCE-1594-1

1.1.8. Hyperlink Security

1.1.8.1. Hyperlink Warnings: Level I

Description
The **DisableHyperLinkWarning** option determines whether Office applications produce a warning when a User clicks a hyperlink or object that links to an executable item.

Rationale
Ensuring that hyperlink warnings are active reduces the attack surface area of the Office system by educating Users to the possibility of potential malicious hyperlinks or objects.

Settings: ..\Microsoft Office 2007 system\Security Settings				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable hyperlink warnings	Disabled	2007	I	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\Security
3. Ensure that the DisableHyperLinkWarning DWORD exists and is set to 0.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
   Microsoft Office 2007 system\Security Settings
3. Double-Click Disable hyperlink warnings.
4. Select Disabled, click OK.

Additional References

CCE-1623-8

1.1.8.2. Hyperlinks in Web Templates: Level II

Description

This option determines whether the File | New and task panes can open template files from Microsoft's Office Online website.

Rationale

Enabling the **DisableTemplatesOnTheWeb** option reduces the attack surface area of the Office system by preventing Users from easily opening potentially malicious files.

Settings: ..\Microsoft Office 2007 system\Miscellaneous				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable hyperlinks to web templates in File | New and task panes	Enabled	2007	II	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\Internet
3. Ensure that the DisableTemplatesOnTheWeb DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Miscellaneous 3. Double-Click Disable hyperlinks to web templates in File | New and task panes. 4. Select Enabled, click OK.

Additional References
CCE-1166-8

1.1.9. External Content Security

1.1.9.1. Warn on Web Beacon in Custom Panel: Level I

Description
This option determines whether Users see a security warning when they open custom Document Information Panels that contain a Web beaconing threat.

Rationale
Web beaconing may send data collected by Document Information Panels to an external server, potentially leaking sensitive information. Setting the **Document Information Panel Beaconing UI** option to **Show UI if XSN is in Internet Zone** will only be prompted about threats if a data transfer is sent to an Internet Zone. This setting provides security while ensuring enterprise application functionality.

Settings: ..\Microsoft Office 2007 system\Document Information Panel				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Document Information Panel Beaconing UI	Enabled Show UI if XSN is in Internet Zone	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\ DocumentInformationPanel 3. Ensure that the Beaconing DWORD exists and is set to 2.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\

Microsoft Office 2007 system\Document Information Panel
3. Double-Click Document Information Panel Beaconing UI.
4. Select Enabled, select Show UI if XSN is in Internet Zone, and click OK.

Additional References
CCE-1505-7

1.1.9.2. Warn on Web Beacon in Custom Panel: Level II

Description
This option determines whether Users see a security warning when they open custom Document Information Panels that contain a Web beaconing threat.

Rationale
Web beaconing may send data collected by Document Information Panels to an external server, potentially leaking sensitive information. Setting the **Document Information Panel Beaconing UI** option to **Always show UI** will always prompt about threats if a data transfer is sent to an Internet Zone. This setting provides maximum security but might hinder enterprise application functionality.

Settings: ..\Microsoft Office 2007 system\Document Information Panel				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Document Information Panel Beaconing UI	Enabled Always show UI	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\ DocumentInformationPanel 3. Ensure that the Beaconing DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Document Information Panel 3. Double-Click Document Information Panel Beaconing UI. 4. Select Enabled, select Always show UI, and click OK.

Additional References
CCE-1505-7

1.1.10. Encryption

1.1.10.1. Encryption Type for Password Protected Office Open XML Files: Level II

Description
The **Encryption type for password protected Office Open XML files** option determines the encryption type used for Open XML files.

Rationale
This configuration, while causing encryption overhead, enforces a more secure encryption algorithm than default settings.

Settings: ..\Microsoft Office 2007 system\Security Settings				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Encryption type for password protected Office Open XML files	Enabled Microsoft Enhanced RSA and AES Cryptographic Provider,AES 256,256	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\Security 3. Ensure that the OpenXMLEncryption SZ exists and is set to Microsoft Enhanced RSA and AES Cryptographic Provider,AES 256,256.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Security Settings 3. Double-Click Encryption type for password protected Office Open XML files. 4. Select Enabled, enter Microsoft Enhanced RSA and AES Cryptographic Provider,AES 256,256, and click OK.

Additional References
CCE-1539-6

1.1.10.2. Encryption for Password Protected Office 97-2003 Files: Level II

Description
The **Encryption type for password protected Office 97-2003 files** option determines the encryption type used for Office 97-2003 files.

Rationale
This configuration, while causing encryption overhead, enforces a more secure encryption algorithm than default settings.

Settings: ..\Microsoft Office 2007 system\Security Settings				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Encryption type for password protected Office 97-2003 files	Enabled Microsoft Enhanced RSA and AES Cryptographic Provider,AES 256,256	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\Security 3. Ensure that the DefaultEncryption DWORD exists and is set to Microsoft Enhanced RSA and AES Cryptographic Provider,AES 256,256.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Security Settings 3. Double-Click Encryption type for password protected Office 97-2003 files. 4. Select Enabled, enter Microsoft Enhanced RSA and AES Cryptographic Provider,AES 256,256, and click OK.

Additional References
CCE-1561-0

1.1.11. Meta-Data Security

1.1.11.1. Protect Document Metadata for Rights in Office Open XML Files: Level I

Description
The **managed Office Open XML Files** option determines whether document metadata is encrypted in password protected Open XML files.

Rationale
Setting this option to **Enabled** will protect against sensitive metadata being stored in plaintext Open XML files even if it is password protected.

Settings: ..\Microsoft Office 2007 system\Security Settings				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Protect document metadata for rights managed Office Open XML Files	Enabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\Security 3. Ensure that the DRMEncryptProperty DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Security Settings 3. Double-Click Protect document metadata for rights managed Office Open XML Files. 4. Select Enabled, click OK.

Additional References
CCE-1508-1

1.1.11.2. Protect Document Metadata or Password Protected Files: Level I

Description
The **Protect document metadata for password protected files** option determines whether document metadata is encrypted in password protected Office documents.

Rationale
Setting this option to **Enabled** will protect against sensitive metadata being stored in plaintext an Office document even if it is password protected.

Settings: ..\Microsoft Office 2007 system\Security Settings				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Protect document metadata for password protected files.	Enabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\Security

3. Ensure that the OpenXMLEncryptProperty DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Security Settings 3. Double-Click Protect document metadata for password protected files.. 4. Select Enabled, click OK.

Additional References
CCE-1640-2

1.1.11.3. Inclusion of Document Properties in PDF and XPS Output: Level II

Description
The **Disable inclusion of document properties in PDF and XPS output** option determines whether document metadata is saved in PDF and XPS formats.

Rationale
Enabling this option protects against the saving and distributing of sensitive metadata in PDF or XPS documents.

Settings: ..\Microsoft Office 2007 system\Microsoft Save As PDF and XPS add-ins				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable inclusion of document properties in PDF and XPS output	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\FixedFormat 3. Ensure that the DisableFixedFormatDocProperties DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Microsoft Save As PDF and XPS add-ins 3. Double-Click Disable inclusion of document properties in PDF and XPS output. 4. Select Enabled, click OK.

Additional References
CCE-1643-6

1.1.12. Miscellaneous

1.1.12.1. Smart Tag Recognition: Level I

Description
The **RecognizeSmartTags** option determines whether Excel will recognize Smart Tags embedded in Excel documents.

Rationale
Smart Tags are executable code, and enabling this functionality will increase the attack surface area of the application. By default, Excel does not recognize Smart Tags, therefore it is recommended to not enable by leaving this setting not-configured.

Settings: ..\Microsoft Office 2007 system\Tools | AutoCorrect Options... (Excel Word PowerPoint and Access)\Smart Tags				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Recognize smart tags in Excel	Not Configured	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Excel\Options 3. Ensure that the RecognizeSmartTags DWORD does not exist.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Tools | AutoCorrect Options... (Excel Word PowerPoint and Access)\Smart Tags 3. Double-Click Recognize smart tags in Excel. 4. Select Not Configured, click OK.

Additional References
CCE-1074-4

1.1.12.2. Configuring Smart Document Manifests: Level II

Description
The **NeverLoadManifests** option determines whether Smart Documents are allowed to install XML expansion packs.

Rationale
Smart Documents are a group of files which include XML schemas, HTML, Word and Excel files. Loading an XML expansion pack file can possibly lead to initialization and loading malicious code. Disabling the use of these expansion packs will prevent negatively affecting the stability of a system which can contribute to data loss.

Settings: ..\Microsoft Office 2007 system\Smart Documents (Word Excel)				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable Smart Document's use of manifests	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\Common\Smart Tag 3. Ensure that the NeverLoadManifests DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Smart Documents (Word Excel) 3. Double-Click Disable Smart Document's use of manifests. 4. Select Enabled, click OK.

Additional References
CCE-903-5

1.1.12.3. Expand Groups in Office when Restricting Permission: Level II

Description
The **Always expand groups in Office when restricting permission for documents** option determines whether groups are expanded to individual User names when applying IRM permissions to Office documents.

Rationale
Setting this option to **Enabled** will protect against a User inadvertently giving read / write permissions to an inappropriate User.

Settings: ..\Microsoft Office 2007 system\Manage Restricted Permissions				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**

Always expand groups in Office when restricting permission for documents	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\DRM\AutoExpandDls 3. Ensure that the AutoExpandDLsEnable DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Manage Restricted Permissions 3. Double-Click Always expand groups in Office when restricting permission for documents. 4. Select Enabled, click OK.

Additional References
CCE-1409-2

1.1.12.4. Microsoft Passport Service for Content using IRM: Level II

Description
The **Disable Microsoft Passport service for content with restricted permission** option determines whether Office applications can connect to a licensing server to verify credentials and determine the IRM access rights assigned to a User for a document signed by a Windows Live ID.

Rationale
Users have the ability to violate governing IRM policies if they are allowed access to external services such as Windows Live ID. Disabling Microsoft Passport service will protect against this policy violation.

Settings: ..\Microsoft Office 2007 system\Manage Restricted Permissions				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable Microsoft Passport service for content with restricted permission	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select:

HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\DRM
3. Ensure that the DisablePassportCertification DWORD exists and is set to 1.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
   Microsoft Office 2007 system\Manage Restricted Permissions
3. Double-Click Disable Microsoft Passport service for content with restricted permission.
4. Select Enabled, click OK.

Additional References

CCE-1237-7

1.1.12.5. Default Program for E-mail, Contacts and Calendar: Level I

Description

This option will determine set Outlook as the default program for e-mail, contacts, and calendar services.

Rationale

Using alternate applications for e-mail, contacts and calendar services may initiate exploitable vulnerabilities by gaining access to sensitive information or launch malicious attacks. Allowing Users to change the default configuration could also enable them to violate organizational policies that govern the use of personal information management software. Enabling this option will protect against the above listed threats.

Settings: ..\microsoft\office\12.0\outlook\options\general

Group Policy Object	Recommended State	Version	Level	Scorability
Make Outlook the default program for E-mail, Contacts, and Calendar	Enabled	2007	I	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:

HKEY_CURRENT_USER\software\policies\microsoft\office\12.0\outlook\options\general
3. Ensure that the Check Default Client DWORD exists and is set to 1.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\Microsoft Office Outlook 2007\Tools |

Options...\Other\ 3. Double-Click Make Outlook the default program for E-mail, Contacts, and Calendar. 4. Select Enabled, click OK.

Additional References
CCE-1111-4

1.1.12.6. Trust E-Mail from Contacts

Description
Setting the **Trust E-mail from Contacts** setting analyzes Users' contacts when filtering junk mail.

Rationale
By setting option to **Enabled**, Outlook will treat Users' contact list as safe senders.

Settings: ..\Microsoft Office Outlook 2007\Tools | Options...\Preferences\Junk E-mail				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Trust E-mail from Contacts	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: Software\Policies\Microsoft\Office\12.0\Outlook\Options

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\Microsoft Office Outlook 2007\Tools | Options...\Preferences\Junk E-mail 3. Double-Click Trust E-mail from Contacts. 4. Select Enabled, click OK.

Additional References
CCE-1117-1

1.1.12.7. Message Format: Level I

Description
Setting the **Message Formats** option specify whether Users apply S/MIME (default), Exchange, Fortezza, S/MIME and Exchange, S/MIME and Fortezza, Exchange and Fortezza, or S/MIME, Exchange, and Fortezza encryption.

Rationale
Setting this option to **Enabled** will protect e-mail sent over open networks by providing end-to-end encryption.

Settings: ..\Software\Policies\Microsoft\Office\12.0\Outlook\Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Message Formats - Support the following message formats: (S/MIME | Exchange | Fortezza | S/MIME and Exchange | S/MIME and Fortezza | Exchange and Fortezza | S/MIME, Exchange, and Fortezza)	Enabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: Software\Policies\Microsoft\Office\12.0\Outlook\Security

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\Microsoft Office Outlook 2007\Security\Cryptography\ 3. Double-Click Message Formats and select the desired form of encryption. 4. Select Enabled, click OK.

Additional References
CCE-1129-6, CCE-1357-3

1.1.12.8. User Configuration to Disable Excel Commands: Level II

Description
The **Disable commands** setting disables specific commands in the interface.

Rationale
Inexperienced or malicious Users may misuse some features of the application to compromise security or cause data loss. Setting this option to **Enabled** will disable some commands.

Settings: ..\ Software\Policies\Microsoft\Office\12.0\Excel\				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**

Disable commands - Review | Changes | Protect and Share Workbook	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: Software\Policies\Microsoft\Office\12.0\Excel\ 3. Ensure that the DisabledCmdBarItemsCheckBoxes DWORD exists and is set to 1

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\Microsoft Office Excel 2007\ 3. Double-Click Disable items in user interface\Predefined\Disable commands - Review | Changes | Protect and Share Workbook 4. Select Enabled, Click OK.

Additional References
CCE-1151-0

1.1.12.9. Rely on VML for displaying graphics in browsers: Level II

Description
The **Rely on VML for displaying graphics in browsers** determines whether Office applications will save copies of VML graphics when documents are saved as web pages.

Rationale
Setting this option to **Disabled** will disallow these graphics to be displayed in non-Microsoft browsers.

Settings: ..\ Software\Policies\Microsoft\Office\12.0\Common\Internet				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Rely on VML for displaying graphics in browsers	Disabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: Software\Policies\Microsoft\Office\12.0\Common\Internet

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\Microsoft Office 2007 system\Tools | Options | General |
3. Double-Click Web Options...\Browsers\Rely on VML for displaying graphics in browsers.
4. Make sure the checkbox is cleared, click OK.

Additional References
CCE-1438-1

1.1.12.10. Prevent users from customizing attachment security settings: Level I

Description
The **Prevent users from customizing attachment security settings** option will disallow Users the ability customize their list of allowed file types.

Rationale
Setting this option to **Enabled** will protect against the introduction of malicious code in Outlook messages.

Settings: ..\Microsoft Office Outlook 2007\Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Prevent users from customizing attachment security settings	Enabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKCU\Software\Policies\Microsoft\Office\12.0\Outlook - 3. Ensure that the DisallowAttachmentCustomization DWORDs exist and are set to 1

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\Microsoft Office Outlook 2007\Security\ 3. Double-Click Prevent users from customizing attachment security settings. 4. Select Enabled, click OK.

Additional References
CCE-1443-1

1.1.12.11. S/MIME password settings: Level I

Description
The **S/MIME password settings** determines how Office stores Key Management Server (KMS) certificates.

Rationale
Maintaining the default configuration of this setting as **Not Configured** will force Outlook to maintain KMS certificates for a minimum duration. This protects against unauthorized access to sensitive information.

Settings: ..\Cryptography\Defaults\Provider\Microsoft Exchange Cryptographic Provider v1.0				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
S/MIME password settings - Default S/MIME password time (minutes): (0 - 2147483647)	Not Configured	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: Software\Policies\Microsoft\Cryptography\Defaults\Provider\Microsoft Exchange Cryptographic Provider v1.0

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\Microsoft Office Outlook 2007\Security\Cryptography\ 3. Double-Click /MIME password settings. 4. Verify that Default S/MIME password time (minutes): (0 - 2147483647) is selected, click OK.

Additional References
CCE-1445-6

1.1.12.12. Hang up when finished sending: Level II

Description
The **Dial-up options** setting determines how Outlook connects to dial-up accounts.

Rationale
The **Hang up when finished sending, receiving, or updating** option disconnects a User

after finishing a manual Send and Receive action, minimizing the amount of time a computer is unnecessarily connected without a User's knowledge.

Settings: ..				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Dial-up options - Hang up when finished sending, receiving, or updating	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\Microsoft Office Outlook 2007\Tools | Options...\Mail Setup\Dial-up options - Hang up when finished sending, receiving, or updating

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: Software\Policies\Microsoft\Office\12.0\Outlook\Options\Mail 3. Double-Click Hang up when finished sending, receiving, or updating. 4. Select Enabled, click OK.

Additional References
CCE-1621-2

1.1.12.13. InfoPath APTCA Assembly Whitelist Enforcement: Level II

Description
The **InfoPath APTCA Assembly Whitelist Enforcement** setting determines whether InfoPath will call assemblies not in the Allowable Assemblies list.

Rationale
By setting this option to **Enabled**, InfoPath 2007 is restricted from calling into any assemblies not in the Allowable Assemblies list. This will protect InfoPath Forms from calling any potentially malicious assemblies in the Global Allowable Cache.

Settings: ..\ Microsoft Office InfoPath 2007 (Machine)\Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
InfoPath APTCA Assembly Whitelist Enforcement	Enabled	2007	II	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   Software\Policies\Microsoft\Office\12.0\InfoPath\Security

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   Computer Configuration\Administrative Templates\Microsoft Office InfoPath 2007 (Machine)\Security\
3. Double-Click InfoPath APTCA Assembly Whitelist Enforcement
4. Select Enabled, click OK.

Additional References

CCE-1739-2

1.1.12.14. Disable user name and password: Level I

Description

The **Disable user name and password** setting determines whether Internet Explorer passes User information such as http://username:password@microsoft.com to Word.

Rationale

Malicious URLs that appear to be legitimate can be constructed and passed to Users in Word. Setting this option to **Enabled** will mitigate this threat by preventing User names and passwords from appearing in URLs

Settings: ..

Group Policy Object	Recommended State	Version	Level	Scorability
Disable user name and password - winword.exe	Enabled	2007	I	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   Software\Policies\Microsoft\Internet Explorer\Main\FeatureControl
3. Ensure that the FEATURE_HTTP_USERNAME_PASSWORD_DISABLE DWORD exists and are set to 1

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   Computer Configuration\Administrative Templates\Microsoft Office 2007 system

(Machine)\Security Settings\IE Security\ 3. Double-Click Disable user name and password. 4. Select winword.exe and Enabled, click OK.

Additional References
CCE-1762-4

1.1.12.15. Only Load Outlook One Off Forms: Level II

Description
The **Allow Active X One Off Forms** setting customizes Outlook 2007's loading of scripts, custom controls, and actions.

Rationale
Setting this option to **Enabled (Load only Outlook Controls)** will prevent malicious third-party scripts, controls and actions from running.

Settings: ..				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Allow Active X One Off Forms	Enabled (Load only Outlook Controls)	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKCU\Software\Policies\Microsoft\Office\12.0\Outlook\Security\ 3. Ensure that the AllowActiveXOneOffForms DWORD exists and are set to 1

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\Classic Administrative Templates\Microsoft Office Outlook 2007\Security\ 3. Double-Click Allow Active X One Off Forms, (Load only Outlook Controls) 4. Select Enabled, click OK.

Additional References
CCE-4280-4

1.1.12.16. Warn before printing, saving or sending a file that contains tracked changes or comments: Level II

Description

The **Warn before printing, saving or sending a file that contains tracked changes or comments** option determines whether a User will be notified with a warning if a file contains tracked changes or comments.

Rationale
Setting this option to **Enabled** will protect against unwanted or sensitive information appearing in documents.

Settings: ..				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Warn before printing, saving or sending a file that contains tracked changes or comments	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKLM\Software\Policies\Microsoft\Office\12.0\Word\Security\Trusted Locations 3. Ensure that the fWarnRevisions_1805_1 DWORD exists and are set to 1

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: Computer Configuration\Administrative Templates\Classic Administrative Templates (ADM)\Microsoft Office Word 2007\Word Options\Security\ 3. Double-Click Warn before printing, saving or sending a file that contains tracked changes or comments. 4. Select Enabled, click OK.

Additional References
CCE-173-5

1.1.12.17. Improve Proofing Tools: Level II

Description
The **Improve Proofing Tools** option determines whether usage data is sent through Microsoft via the Help Improve Proofing Tools feature.

Rationale
Setting this option to **Disabled** will protect against content sent to Microsoft that may contain sensitive information if the Proofing Tool marks words as misspelled or phrases as containing improper grammar.

Settings: ..\Microsoft Office 2007 system\Tools | Options | Spelling\Proofing Data Collection				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Improve Proofing Tools	Disabled	2007	II	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\PTWatson
3. Ensure that the PTWOptIn DWORD exists and is set to 0.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
   Microsoft Office 2007 system\Tools | Options | Spelling\Proofing Data Collection
3. Double-Click Improve Proofing Tools.
4. Select Disabled, click OK.

Additional References

CCE-1292-2

1.1.12.18. Automatically Receive Small Updates: Level II

Description

The **Automatically receive small updates to improve reliability** option determines whether Microsoft Office Diagnostics is enabled.

Rationale

Applying updates without testing may result in reduced availability of applications installed on core enterprise infrastructure and can also lead to divergent configuration schemes on various machines. Many enterprise level environments have patch management teams and mechanisms such as Intrusion Prevention Systems that help mitigate the risk of enterprise systems that have not been updated for the short interim of testing before updates are rolled out.

Settings: ..\Microsoft Office 2007 system\Privacy\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Automatically receive small updates to improve reliability	Disabled	2007	II	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\General
3. Ensure that the UpdateReliabilityData DWORD exists and is set to 0.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
      Microsoft Office 2007 system\Privacy\Trust Center
3. Double-Click Automatically receive small updates to improve reliability.
4. Select Disabled, click OK.

Additional References

CCE-276-6

1.1.12.19. Trust Bar Notifications: Level I

Description

The **Disable all Trust Bar notifications for security issues** option determines whether Users are notified in the event of a security issue via the Trust Bar.

Rationale

Disabling this option allows a User to properly assess the security posture of a document via the Trust Bar.

Settings: ..\Microsoft Office 2007 system\Security Settings

Group Policy Object	Recommended State	Version	Level	Scorability
Disable all Trust Bar notifications for security issues	Disabled	2007	I	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\TrustCenter
3. Ensure that the TrustBar DWORD exists and is set to 0.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
      Microsoft Office 2007 system\Security Settings
3. Double-Click Disable all Trust Bar notifications for security issues.

4. Select Disabled, click OK.

Additional References
CCE-1486-0

1.1.12.20. Mix of Policy and User Locations: Level I

Description
The **Allow mix of policy and User locations** option determines whether a trusted location can be defined by the Group Policy, a User, or the Office Customization Tool.

Rationale
Setting this option to **Disabled** prevents a User from creating a potentially insecure custom trusted location.

Settings: ..\Microsoft Office 2007 system\Security Settings\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Allow mix of policy and User locations	Disabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\Security\Trusted Locations 3. Ensure that the Allow User Locations DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Security Settings\Trust Center 3. Double-Click Allow mix of policy and User locations. 4. Select Disabled, click OK.

Additional References
CCE-770-8

1.2. Outlook

1.2.1. Attachment Security

1.2.1.1. Attachment Saving Temporary Folder: Level I

Description
The **Attachment Secure Temporary Folder** option allows an administrator to specify a particular folder instead of defaulting to a randomly generated name for the temporary saving of attachment files opened in Outlook.

Rationale
Setting this option to **Disabled** will protect against a malicious User or code attempting to gain access to User attachments by targeting files saved in the same predictable location.

Settings: ..\Microsoft Office Outlook 2007\Security\Cryptography\Signature Status dialog box

Group Policy Object	Recommended State	Version	Level	Scorability
Attachment Secure Temporary Folder	Disabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the OutlookSecureTempFolder DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Cryptography\Signature Status dialog box 3. Double-Click Attachment Secure Temporary Folder. 4. Select Disabled, click OK.

Additional References
CCE-1591-7

1.2.1.2. Attachment Previewing in Outlook: Level II

Description
The **Do not allow attachment previewing in Outlook** option determines whether attachments can be previewed in Outlook.

Rationale
Enabling this option reduces the attack surface area of Outlook.

Settings: ..\Microsoft Office Outlook 2007\Tools | Options...\Preferences\E-mail Options				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Do not allow attachment previewing in Outlook	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Preferences 3. Ensure that the DisableAttachmentPreviewing DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Tools | Options...\Preferences\E-mail Options 3. Double-Click Do not allow attachment previewing in Outlook. 4. Select Enabled, click OK.

Additional References
CCE-1192-4

1.2.1.3. Block Potentially Dangerous Attachments: Level I

Description
The **Display Level 1 attachments** option determines whether Outlook blocks potentially dangerous attachments.

Rationale
Setting this option to **Disabled** prevents potentially dangerous attachments from being opened under all circumstances.

Settings: ..\Microsoft Office Outlook 2007\Security\Security Form Settings\Attachment Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Display Level 1 attachments	Disabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK.

2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security
3. Ensure that the ShowLevel1Attach DWORD exists and is set to 0.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
      Microsoft Office Outlook 2007\Security\Security Form Settings\Attachment Security
3. Double-Click Display Level 1 attachments.
4. Select Disabled, click OK.

Additional References

CCE-1296-3

1.2.1.4. Block Potentially Dangerous Attachments: Level II

Description

The **Allow Users to demote attachments to Level 2** option determines whether a User can set a registry setting to demote certain attachment types to Level 2, in order to save them to disk and then open them.

Rationale

Setting this option to **Disabled** demotes Level 1 attachments, which may contain malicious code or functionality that can be harmful to a User's computer or data, to Level 2.

Settings: ..\Microsoft Office Outlook 2007\Security\Security Form Settings\Attachment Security

Group Policy Object	Recommended State	Version	Level	Scorability
Allow Users to demote attachments to Level 2	Disabled	2007	I	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security
3. Ensure that the AllowUsersToLowerAttachments DWORD exists and is set to 0.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
      Microsoft Office Outlook 2007\Security\Security Form Settings\Attachment Security
3. Double-Click Allow Users to demote attachments to Level 2.

4. Select Disabled, click OK.

Additional References
CCE-1388-8

1.2.1.5. Add File Extension to Block as Level 1: Level I

Description
The **Add file extensions to block as Level 1** option determines types of attachments, determined by extension, which may not be opened by Users.

Rationale
This option is used by enterprise administrators to specify file types that cannot be opened from Outlook.

Settings: ..\Microsoft Office Outlook 2007\Security\Security Form Settings\Attachment Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Add file extensions to block as Level 1	Not Configured	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the FileExtensionsAddLevel1 DWORD does not exist.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Security Form Settings\Attachment Security 3. Double-Click Add file extensions to block as Level 1. 4. Select Not Configured, click OK.

Additional References
CCE-1617-0

1.2.1.6. Add File Extension to Block as Level 2: Level I

Description
The **Add file extensions to block as Level 2** option determines types of attachments, determined by extension, which may not be opened by Users.

Rationale
This option is informational is used by enterprise administrators to specify file types that cannot be opened from Outlook.

Settings: ..\Microsoft Office Outlook 2007\Security\Security Form Settings\Attachment Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Add file extensions to block as Level 2	Not Configured	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the FileExtensionsAddLevel2 DWORD does not exist.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Security Form Settings\Attachment Security 3. Double-Click Add file extensions to block as Level 2. 4. Select Not Configured, click OK.

Additional References
CCE-1155-1

1.2.1.7. Remove File Extensions Blocked as Level 1: Level I

Description
The **Remove file extensions blocked as Level 1** option determines whether administrators can remove attachment types, listed by file name extension, from the block list.

Rationale
Setting this option to **Disabled** will protect Users against opening potentially harmful file types without a warning prompt for types that would otherwise have been blocked from opening.

Settings: ..\Microsoft Office Outlook 2007\Security\Security Form Settings\Attachment Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Remove file extensions blocked as Level 1	Disabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the FileExtensionsRemoveLevel1 DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Security Form Settings\Attachment Security 3. Double-Click Remove file extensions blocked as Level 1. 4. Select Disabled, click OK.

Additional References
CCE-1631-1

1.2.1.8. Remove File Extensions Blocked as Level 2: Level I

Description
The **Remove file extensions blocked as Level 2** option determines whether administrators can remove attachment types, listed by file name extension, from the block list.

Rationale
Setting this option to Disabled will protect from Users to saving and opening potentially harmful file types without a warning prompt.

Settings: ..\Microsoft Office Outlook 2007\Security\Security Form Settings\Attachment Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Remove file extensions blocked as Level 2	Disabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the FileExtensionsRemoveLevel2 DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select:

User Configuration\Administrative Templates\
Microsoft Office Outlook 2007\Security\Security Form Settings\Attachment Security
3. Double-Click Remove file extensions blocked as Level 2.
4. Select Disabled, click OK.

Additional References
CCE-1556-0

1.2.1.9. Download Full Text of Articles as HTML Attachments: Level I

Description
The **Download full text of articles as HTML attachments** option determines whether full text RSS entries are downloaded as HTML attachments in Outlook.

Rationale
Setting this option to **Disabled** prevents Outlook from frequently updating or downloading very large messages, reducing the attack surface of Outlook.

Settings: ..\Microsoft Office Outlook 2007\Tools | Account Settings\RSS Feeds				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Download full text of articles as HTML attachments	Disabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Options\RSS 3. Ensure that the EnableFullTextHTML DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Tools | Account Settings\RSS Feeds 3. Double-Click Download full text of articles as HTML attachments. 4. Select Disabled, click OK.

Additional References
CCE-1311-0

1.2.1.10. Automatically Download Attachments: Level II

Description
The **Automatically download attachments** Outlook setting determines whether automatically

attachments are automatically downloaded for Internet Calendar appointments.

Rationale
Setting this option to **Disabled** protects against the download of files attached to Internet Calendar appointments that may contain malicious code that may compromise a computer.

Settings: ..\Microsoft Office Outlook 2007\Tools | Account Settings\Internet Calendars				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Automatically download attachments	Disabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Options\WebCal 3. Ensure that the EnableAttachments DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Tools | Account Settings\Internet Calendars 3. Double-Click Automatically download attachments. 4. Select Disabled, click OK.

Additional References
CCE-1682-4

1.2.2. S/MIME

1.2.2.1. Store Password Information for Least Possible Time: Level II

Description
This option determines the length of time in minutes that Outlook stores password information for Key Management Service (KMS) certificates.

Rationale
Setting the minimum value (1 minute) in which Outlook will cache KMS passwords reduces the risk of malicious User using cached credentials to read encrypted e-mail on a User's computer.

Settings: ..\Microsoft Office Outlook 2007\Security\Cryptography

Group Policy Object	Recommended State	Version	Level	Scorability
S/MIME password settings	Enabled 1	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Cryptography\Defaults\Provider 3. Ensure that the Microsoft Exchange Cryptographic Provider v1.0 DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Cryptography 3. Double-Click S/MIME password settings. 4. Select Enabled, select 1, and click OK.

Additional References
CCE-1163-5

1.2.3. RPC Security

1.2.3.1. Enabling RPC Encryption: Level I

Description
The **EnableRPCEncryption** option controls whether Outlook uses RPC encryption to communicate with Microsoft Exchange servers.

Rationale
Enabling encryption prevents data from being read or modified in between the Outlook client and the Exchange server.

Settings: ..\Microsoft Office Outlook 2007\Tools | Account Settings\Exchange				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Enable RPC encryption	Enabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\RPC 3. Ensure that the EnableRPCEncryption DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Tools | Account Settings\Exchange 3. Double-Click Enable RPC encryption. 4. Select Enabled, click OK.

Additional References
CCE-1082-7

1.2.4. Authentication

1.2.4.1. Exchange Server Authentication: Level I

Description
This option controls the authentication mechanism Outlook uses to authenticate to an Exchange Server.

Rationale
Kerberos is the preferred authentication mechanism because is the strongest algorithm supported by Outlook to authenticate to an Exchange server. If Kerberos is not supported, Outlook will attempt authentication using NTLM.

Settings: ..\Microsoft Office Outlook 2007\Tools | Account Settings\Exchange				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Authentication with Exchange Server	Enabled Kerberos/NTLM Password Authentication	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the AuthenticationService DWORD exists and is set to 9.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Tools | Account Settings\Exchange 3. Double-Click Authentication with Exchange Server.

4. Select Enabled, select Kerberos/NTLM Password Authentication, and click OK.

Additional References
CCE-1712-9

1.2.5. Public / Shared Folder Security

1.2.5.1. Scripts for Shared Folders: Level I

Description
This option controls whether Outlook executes scripts that are associated with custom forms or folder home pages for public folders.

Rationale
Enabling the **SharedFolderScript** option disables browsed to shared folders that may contain malicious scripts from automatically executing.

Settings: ..\Microsoft Office Outlook 2007\Tools | Options...\Other\Advanced				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Do not allow Outlook object model scripts to run for shared folders	Enabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the SharedFolderScript DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Tools | Options...\Other\Advanced 3. Double-Click Do not allow Outlook object model scripts to run for shared folders. 4. Select Enabled, click OK.

Additional References
CCE-1529-7

1.2.5.2. Non-Default Folders as Folder Home Pages: Level II

Description
The **Do not allow folders in non-default stores to be set as folder home pages** option determines whether a User can configure a folder home page for folders in non-default

stores.

Rationale
Setting this option to **Enabled** reduces the attack surface of Outlook by not allowing scripts which may be included in web pages that access the Outlook object model.

Settings: ..\Microsoft Office Outlook 2007\Tools | Options...\Other\Advanced				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Do not allow folders in non-default stores to be set as folder home pages	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the NonDefaultStoreScript DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Tools | Options...\Other\Advanced 3. Double-Click Do not allow folders in non-default stores to be set as folder home pages. 4. Select Enabled, click OK.

Additional References
CCE-1494-4

1.2.5.3. Run Outlook Object Model Scripts for Public Folders: Level I

Description
The **Do not allow Outlook object model scripts to run for public folders** option controls whether Outlook executes Outlook object model scripts that are associated with custom forms or folder home pages for public folders.

Rationale
Setting this option to **Enabled** disallows browsed to Shared folders which contain malicious scripts from automatically executing.

Settings: ..\Microsoft Office Outlook 2007\Tools | Options...\Other\Advanced				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**

Do not allow Outlook object model scripts to run for public folders	Enabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the PublicFolderScript DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Tools | Options...\Other\Advanced 3. Double-Click Do not allow Outlook object model scripts to run for public folders. 4. Select Enabled, click OK.

Additional References
CCE-1560-2

1.2.5.4. Configure Outlook Object Model when Sending Mail: Level I

Description
The **Configure Outlook object model prompt when sending mail** option determines the action Outlook performs when an untrusted program tries to programmatically send e-mail.

Rationale
Setting this option to **Prompt User based on computer security** will mitigate programmatic access to this functionality could allow the propagation of worms, impersonation the User, and launching of Denial of Service attacks.

Settings: ..\Microsoft Office Outlook 2007\Security\Security Form Settings\Programmatic Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Configure Outlook object model prompt when sending mail	Enabled Prompt User based on computer security	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the PromptOOMSend DWORD exists and is set to 3.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Security Form Settings\Programmatic Security 3. Double-Click Configure Outlook object model prompt when sending mail. 4. Select Enabled, select Prompt User based on computer security, click OK.

Additional References
CCE-1590-9

1.2.5.5. Configure Outlook Object Model when Sending Mail: Level II

Description
The **Configure Outlook object model prompt when sending mail** option determines the action Outlook performs when an untrusted program tries to programmatically send e-mail.

Rationale
Setting this option to **Automatically Deny** will disallow programmatic access to this functionality could allow the propagation of worms, impersonation the User, and launching of Denial of Service attacks.

Settings: ..\Microsoft Office Outlook 2007\Security\Security Form Settings\Programmatic Security

Group Policy Object	Recommended State	Version	Level	Scorability
Configure Outlook object model prompt when sending mail	Enabled Automatically Deny	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the PromptOOMSend DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Security Form Settings\Programmatic Security 3. Double-Click Configure Outlook object model prompt when sending mail. 4. Select Enabled, select Automatically Deny, and click OK.

Additional References
CCE-1590-9

1.2.5.6. Outlook Object Model when Accessing Address Book: Level I

Description
The **Configure Outlook object model prompt when accessing an address book** option determines how Outlook handles a program programmatically gaining access address book items.

Rationale
Allowing programmatic access to this functionality could access to sensitive data may be used to propagate worms. Setting this option to **Enabled** prompts a User when using the "Programmatic Access" Trust Center settings.

Settings: ..\Microsoft Office Outlook 2007\Security\Security Form Settings\Programmatic Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Configure Outlook object model prompt when accessing an address book	Enabled Prompt User based on computer security	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the PromptOOMAddressBookAccess DWORD exists and is set to 3.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Security Form Settings\Programmatic Security 3. Double-Click Configure Outlook object model prompt when accessing an address book. 4. Select Enabled, select Prompt User based on computer security, click OK.

Additional References
CCE-1004-1

1.2.5.7. Outlook Object Model when Accessing Address Book: Level II

Description

The **Configure Outlook object model prompt when accessing an address book** option determines how Outlook handles a program programmatically gaining access address book items.

Rationale
Allowing programmatic access to this functionality could allow the program access to sensitive data which could be used to propagate worms. Setting this option to **Enabled** produces a prompt when any program attempts to programmatically access an address book.

Settings: ..\Microsoft Office Outlook 2007\Security\Security Form Settings\Programmatic Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Configure Outlook object model prompt when accessing an address book	Enabled Automatically Deny	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the PromptOOMAddressBookAccess DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Security Form Settings\Programmatic Security 3. Double-Click Configure Outlook object model prompt when accessing an address book. 4. Select Enabled, select Automatically Deny, and click OK.

Additional References
CCE-1004-1

1.2.5.8. Configure Outlook Object Model when Reading Address: Level I

Description
The **Configure Outlook object model prompt when reading address information** option determines how Outlook responds to a program programmatically attempting to access Recipient.

Rationale
Programmatic access allows a program to modify the Recipient, potentially sending sensitive data to a malicious User. Setting this option to **Prompt User based on computer security**

prompts a User if antivirus software is turned off or not up to date.

Settings: ..\Microsoft Office Outlook 2007\Security\Security Form Settings\Programmatic Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Configure Outlook object model prompt when reading address information	Enabled Prompt User based on computer security	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the PromptOOMAddressInformationAccess DWORD exists and is set to 3.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Security Form Settings\Programmatic Security 3. Double-Click Configure Outlook object model prompt when reading address information. 4. Select Enabled, select Prompt User based on computer security, click OK.

Additional References
CCE-1273-2

1.2.5.9. Configure Outlook Object Model when Reading Address: Level II

Description
The **Configure Outlook object model prompt when reading address information** option determines how Outlook responds to a program programmatically attempting to access Recipient.

Rationale
Programmatic access allows a program to modify the Recipient, potentially sending sensitive data to a malicious User. Setting this option to **Automatically Deny** will not permit a program to make programmatic requests.

Settings: ..\Microsoft Office Outlook 2007\Security\Security Form Settings\Programmatic Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**

Configure Outlook object model prompt when reading address information	Enabled Automatically Deny	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the PromptOOMAddressInformationAccess DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Security Form Settings\Programmatic Security 3. Double-Click Configure Outlook object model prompt when reading address information. 4. Select Enabled, select Automatically Deny, and click OK.

Additional References
CCE-1273-2

1.2.5.10. Configure Outlook Object Model when Responding: Level I

Description
The **Configure Outlook object model prompt when responding to meeting and task requests** option determines how Outlook responds to a program attempts to programmatically reply to a meeting or task request item.

Rationale
Allowing programmatic access to the reply functionality could allow a malicious User to impersonate the User. Setting this option to **Prompt User based on computer security** prompts a User if antivirus software is turned off or not up to date.

Settings: ..\Microsoft Office Outlook 2007\Security\Security Form Settings\Programmatic Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Configure Outlook object model prompt when responding to meeting and task requests	Enabled Prompt User based on computer security	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK.

2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security
3. Ensure that the PromptOOMMeetingTaskRequestResponse DWORD exists and is set to 3.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
      Microsoft Office Outlook 2007\Security\Security Form Settings\Programmatic Security
3. Double-Click Configure Outlook object model prompt when responding to meeting and task requests.
4. Select Enabled, select Prompt User based on computer security, click OK.

Additional References

CCE-1172-6

1.2.5.11. Configure Outlook Object Model when Responding: Level II

Description

The **Configure Outlook object model prompt when responding to meeting and task requests** option determines how Outlook responds to a program attempts to programmatically reply to a meeting or task request item.

Rationale

Allowing programmatic access to the reply functionality could allow a malicious User to impersonate the User. Setting this option to **Automatically Deny** will not permit a program to make programmatic requests.

Settings: ..\Microsoft Office Outlook 2007\Security\Security Form Settings\Programmatic Security

Group Policy Object	Recommended State	Version	Level	Scorability
Configure Outlook object model prompt when responding to meeting and task requests	Enabled Automatically Deny	2007	II	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security
3. Ensure that the PromptOOMMeetingTaskRequestResponse DWORD exists and is set to 0.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
      Microsoft Office Outlook 2007\Security\Security Form Settings\Programmatic Security
3. Double-Click Configure Outlook object model prompt when responding to meeting and task requests.
4. Select Enabled, select Automatically Deny, and click OK.

Additional References
CCE-1172-6

1.2.5.12. Configure Outlook Object Model when Executing Save As: Level I

Description
The **Configure Outlook object model prompt when executing Save As** option determines how Outlook responds a untrusted program attempts to programmatically access the Save As command.

Rationale
If an untrusted application uses the Save As command to programmatically save an item, the application could add malicious data to a User's inbox, a public folder, or an address book. Setting this option to **Prompt User based on computer security** prompts a User if antivirus software is turned off or not up to date.

Settings: ..\Microsoft Office Outlook 2007\Security\Security Form Settings\Programmatic Security

Group Policy Object	Recommended State	Version	Level	Scorability
Configure Outlook object model prompt when executing Save As	Enabled Prompt User based on computer security	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the PromptOOMSaveAs DWORD exists and is set to 3.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Security Form Settings\Programmatic Security

3. Double-Click Configure Outlook object model prompt when executing Save As. 4. Select Enabled, select Prompt User based on computer security, click OK.

Additional References
CCE-1568-5

1.2.5.13. Configure Outlook Object Model when Executing Save As: Level II

Description
The **Configure Outlook object model prompt when executing Save As** option determines how Outlook responds a untrusted program attempts to programmatically access the Save As command.

Rationale
If an untrusted application uses the Save As command to programmatically save an item, the application could add malicious data to a User's inbox, a public folder, or an address book. Setting this option to **Automatically Deny** will not permit a program to make programmatic requests.

Settings: ..\Microsoft Office Outlook 2007\Security\Security Form Settings\Programmatic Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Configure Outlook object model prompt when executing Save As	Enabled Automatically Deny	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the PromptOOMSaveAs DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Security Form Settings\Programmatic Security 3. Double-Click Configure Outlook object model prompt when executing Save As. 4. Select Enabled, select Automatically Deny, and click OK.

Additional References
CCE-1568-5

1.2.5.14. Configure Outlook Object Model when Accessing Formula: Level I

Description
The **Configure Outlook object model prompt When accessing the Formula property of a UserProperty object** option determines the Outlook a User opening or creating a custom form that binds an Address Information field to a combination or formula custom field.

Rationale
If an untrusted application gains access to Address Information, it could be used to compromise sensitive information or propagate worms. Setting this option to **Prompt User based on computer security** prompts a User if antivirus software is turned off or not up to date.

Settings: ..\Microsoft Office Outlook 2007\Security\Security Form Settings\Programmatic Security

Group Policy Object	Recommended State	Version	Level	Scorability
Configure Outlook object model prompt When accessing the Formula property of a UserProperty object	Enabled Prompt User based on computer security	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the PromptOOMFormulaAccess DWORD exists and is set to 3.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Security Form Settings\Programmatic Security 3. Double-Click Configure Outlook object model prompt When accessing the Formula property of a UserProperty object. 4. Select Enabled, select Prompt User based on computer security, click OK.

Additional References
CCE-1573-5

1.2.5.15. Configure Outlook Object Model when Accessing Formula: Level II

Description
The **Configure Outlook object model prompt When accessing the Formula property of a UserProperty object** option determines the Outlook a User opening or creating a custom form

that binds an Address Information field to a combination or formula custom field.

Rationale
If an untrusted application gains access to Address Information, it could be used to compromise sensitive information or propagate worms. Setting this option to **Automatically Deny** will not permit a program to make programmatic requests.

Settings: ..\Microsoft Office Outlook 2007\Security\Security Form Settings\Programmatic Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Configure Outlook object model prompt When accessing the Formula property of a UserProperty object	Enabled Automatically Deny	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the PromptOOMFormulaAccess DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Security Form Settings\Programmatic Security 3. Double-Click Configure Outlook object model prompt When accessing the Formula property of a UserProperty object. 4. Select Enabled, select Automatically Deny, and click OK.

Additional References
CCE-1573-5

1.2.5.16. Configure Outlook Object Model when Accessing Address: Level I

Description
The **Configure Outlook object model prompt when accessing address information via UserProperties.Find** option determines how Outlook handles Address Information accessed by the UserProperties.Find method.

Rationale
If an untrusted application gains access to Address Information, it could be used to compromise sensitive information or propagate worms. Setting this option to **Prompt User**

based on computer security prompts a User if antivirus software is turned off or not up to date.

Settings: ..\Microsoft Office Outlook 2007\Security\Security Form Settings\Programmatic Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Configure Outlook object model prompt when accessing address information via UserProperties.Find	Enabled Prompt User based on computer security	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the PromptOOMAddressUserPropertyFind DWORD exists and is set to 3.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Security Form Settings\Programmatic Security 3. Double-Click Configure Outlook object model prompt when accessing address information via UserProperties.Find. 4. Select Enabled, select Prompt User based on computer security, click OK.

Additional References
CCE-1454-8

1.2.5.17. Configure Outlook Object Model when Accessing Address: Level II

Description
The **Configure Outlook object model prompt when accessing address information via UserProperties.Find** option determines how Outlook handles Address Information accessed by the UserProperties.Find method.

Rationale
If an untrusted application gains access to Address Information, it could be used to compromise sensitive information or propagate worms. Setting this option to **Automatically Deny** will not permit a program to make programmatic requests.

Settings: ..\Microsoft Office Outlook 2007\Security\Security Form Settings\Programmatic Security

Group Policy Object	Recommended State	Version	Level	Scorability
Configure Outlook object model prompt when accessing address information via UserProperties.Find	Enabled Automatically Deny	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the PromptOOMAddressUserPropertyFind DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Security Form Settings\Programmatic Security 3. Double-Click Configure Outlook object model prompt when accessing address information via UserProperties.Find. 4. Select Enabled, select Automatically Deny, and click OK.

Additional References
CCE-1454-8

1.2.6. Certificate Security

1.2.6.1. Check E-mail Address against Certificates: Level I

Description
This option controls whether Outlook verifies the User's e-mail address with the address associated with the certificate used for signing.

Rationale
If a User's e-mail address does not match the address associated with the certificate used for signing, an error may occur when the receipt attempts to read the message or verify the signature.

Settings: ..\Microsoft Office Outlook 2007\Security\Cryptography				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Do not check e-mail address against address of certificates being used	Disabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the SupressNameChecks DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Cryptography 3. Double-Click Do not check e-mail address against address of certificates being used. 4. Select Disabled, click OK.

Additional References
CCE-316-0

1.2.6.2. Warn on Missing Root Certificates: Level I

Description
The **SigStatusNoTrustDecision** option controls how Outlook functions when a root certificate is missing. By default, if a root certificate is trusted, then all certificates issued by the Certificate Authority will subsequently be trusted.

Rationale
A root certificate will not validate against the Certificate Authority and is no longer trusted if it is compromised. Enabling this option ensures that Users are notified when there is an issue with the root certificate.

Settings: ..\Microsoft Office Outlook 2007\Security\Cryptography\Signature Status dialog box

Group Policy Object	Recommended State	Version	Level	Scorability
Missing root certificates	Enabled warning	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the SigStatusNoTrustDecision DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK.

2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Cryptography\Signature Status dialog box 3. Double-Click Missing root certificates. 4. Select Enabled, select warning, and click OK.

Additional References
CCE-1076-9

1.2.7. Encryption

1.2.7.1. Minimum Encryption Settings: Level I

Description
This option allows administrators to set a minimum key size for encrypting e-mail messages sent from Outlook.

Rationale
128 bit keys are the minimum industry standard for encryption and offer a moderate amount of security without a large encryption overhead.

Settings: ..\Microsoft Office Outlook 2007\Security\Cryptography				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Minimum encryption settings	Enabled 128	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the MinEncKey DWORD exists and is set to 80.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Cryptography 3. Double-Click Minimum encryption settings. 4. Select Enabled, select 128, and click OK.

Additional References
CCE-13-3

1.2.7.2. Minimum Encryption Settings: Level II

Description
This option allows administrators to set a minimum key size for encrypting e-mail messages sent from Outlook.

Rationale
256 bit keys offer more security than 128 bit keys, but incur a larger encryption overhead.

Settings: ..\Microsoft Office Outlook 2007\Security\Cryptography				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Minimum encryption settings	Enabled 256	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the MinEncKey DWORD exists and is set to 100.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Cryptography 3. Double-Click Minimum encryption settings. 4. Select Enabled, select 256, and click OK.

Additional References
CCE-13-3

1.2.7.3. Sending of E-mails after Encryption Warning: Level II

Description
This option controls whether Outlook Users are allowed to send e-mail messages after they are presented with an encryption warning.

Rationale
Users may bypass security settings set by the system administrator if they are allowed to send e-mail messages after receiving an encryption warning. Enabling this option will not allow Users to select *Continue* on encryption warning dialog boxes.

Settings: ..\Microsoft Office Outlook 2007\Security\Cryptography

Group Policy Object	Recommended State	Version	Level	Scorability
Do not provide Continue option on Encryption warning dialog boxes	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the DisableContinueEncryption DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Cryptography 3. Double-Click Do not provide Continue option on Encryption warning dialog boxes. 4. Select Enabled, click OK.

Additional References
CCE-1511-5

1.2.7.4. Sign All Outgoing E-mail Messages: Level II

Description
This option controls whether digital signatures are required on all outgoing e-mail messages in Outlook 2007.

Rationale
Signed e-mail messages assure a Recipient of the Sender's authenticity. Enabling this option may potentially disable e-mail services for a User who does not have valid a digital signature for signing e-mail messages.

Settings: ..\Microsoft Office Outlook 2007\Security\Cryptography				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Sign all e-mail messages	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the AlwaysSign DWORD exists and is set to 1.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
   Microsoft Office Outlook 2007\Security\Cryptography
3. Double-Click Sign all e-mail messages.
4. Select Enabled, click OK.

Additional References
CCE-1639-4

1.2.7.5. Invalid Digital Signature Warning: Level I

Description
Enabling this option warns Outlooks Users about messages with invalid digital signatures.

Rationale
Users warned about invalid signatures will prevent against the deceptive use of invalid signatures.

Settings: ..\Microsoft Office Outlook 2007\Security\Cryptography				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Signature Warning	Enabled Always warn about invalid signatures	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the WarnAboutInvalid DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Cryptography 3. Double-Click Signature Warning. 4. Select Enabled, select Always warn about invalid signatures, click OK.

Additional References
CCE-700-5

1.2.8. UI Customization Security

1.2.8.1. Set Control ItemProperty Prompt: Level I

Description
The **Set control ItemProperty prompt** setting determines how Outlook handles opening forms with controls bound to Address Information fields.

Rationale
Setting this option to **Prompt User based on computer security** prompts a User if antivirus software is turned off or not up to date. This option controls access to Address Information fields which prevents worms from easily propagating, but may introduce usability issues.

Settings: ..\Microsoft Office Outlook 2007\Security\Security Form Settings\Custom Form Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Set control ItemProperty prompt	Enabled Prompt User based on computer security	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the PromptOOMItemPropertyAccess DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Security Form Settings\Custom Form Security 3. Double-Click Set control ItemProperty prompt. 4. Select Enabled, select Prompt User based on computer security, click OK.

Additional References
CCE-1586-7

1.2.8.2. Set Control ItemProperty Prompt: Level II

Description
The **Set control ItemProperty prompt** setting determines how Outlook handles opening forms with controls bound to Address Information fields.

Rationale
Setting this option to **Automatically Deny** will restrict access to Address Information fields which prevents worms from easily propagating.

Settings: ..\Microsoft Office Outlook 2007\Security\Security Form Settings\Custom Form Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Set control ItemProperty prompt	Enabled Automatically Deny	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the PromptOOMItemPropertyAccess DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Security Form Settings\Custom Form Security 3. Double-Click Set control ItemProperty prompt. 4. Select Enabled, select Automatically Deny, and click OK.

Additional References
CCE-1586-7

1.2.9. Object Model Guard Settings

1.2.9.1. Outlook Object Model Custom Actions Execution Prompt: Level I

Description
The **Set Outlook object model Custom Actions execution prompt** setting determines how Outlook prompts a User before the execution of custom actions.

Rationale
As part of a rule, custom actions may be triggered which can potentially evade controls that protect against the programmatic sending of e-mail, thereby allowing the action to send sensitive data or malicious code to another User. Setting the **Prompt User based on computer security** option to **Enabled** is Outlook's default configuration.

Settings: ..\Microsoft Office Outlook 2007\Security\Security Form Settings\Custom Form Security

Group Policy Object	Recommended State	Version	Level	Scorability
Set Outlook object model Custom Actions execution prompt	Enabled Prompt User based on computer security	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the PromptOOMCustomAction DWORD exists and is set to 3.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Security Form Settings\Custom Form Security 3. Double-Click Set Outlook object model Custom Actions execution prompt. 4. Select Enabled, select Prompt User based on computer security, click OK.

Additional References
CCE-1436-5

1.2.9.2. Outlook Object Model Custom Actions Execution Prompt: Level II

Description
The **Set Outlook object model Custom Actions execution prompt** setting determines how Outlook prompts a User before the execution of custom actions.

Rationale
As part of a rule, custom actions may be triggered which can potentially evade controls that protect against the programmatic sending of e-mail, thereby allowing the action to send sensitive data or malicious code to another User. Setting this option to **Automatically Deny** will deny all custom actions that use the Outlook object model from executing.

Settings: ..\Microsoft Office Outlook 2007\Security\Security Form Settings\Custom Form Security

Group Policy Object	Recommended State	Version	Level	Scorability
Set Outlook object model Custom Actions execution prompt	Enabled Automatically Deny	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK.

2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security
3. Ensure that the PromptOOMCustomAction DWORD exists and is set to 0.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
   Microsoft Office Outlook 2007\Security\Security Form Settings\Custom Form Security
3. Double-Click Set Outlook object model Custom Actions execution prompt.
4. Select Enabled, select Automatically Deny, and click OK.

Additional References

CCE-1436-5

1.2.10. Add-In Security

1.2.10.1. Configure Trusted Add-Ins: Level I

Description

The **Configure trusted add-ins** option determines whether Outlook allows add-ins configured as trusted to be allowed to run without the normal add-in security measures.

Rationale

Setting this option to **Disabled** will not allow add-ins without security measures, which could potentially lead to the execution of malicious code and the compromise of a User's machine and data, to run.

Settings: ..\Microsoft Office Outlook 2007\Security\Security Form Settings\Programmatic Security\Trusted Add-ins

Group Policy Object	Recommended State	Version	Level	Scorability
Configure trusted add-ins	Disabled	2007	II	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security
3. Ensure that the TrustedAddins DWORD exists and is set to 0.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\

Microsoft Office Outlook 2007\Security\Security Form Settings\Programmatic Security\Trusted Add-ins 3. Double-Click Configure trusted add-ins. 4. Select Disabled, click OK.

Additional References
CCE-786-4

1.2.11. External Content Security

1.2.11.1. Block Automatic Download of External Content: Level I

Description
The **Display pictures and external content in HTML e-mail** option determines if Outlook automatically downloads and displays external content, such as a web beacon, in HTML e-mail.

Rationale
Malicious e-mail Senders can send HTML e-mail messages with embedded Web beacons. If a User views a malicious e-mail with an embedded web beacon, it may provide confirmation to the Sender that the Recipient's e-mail address is legitimate. Setting this option to **Disabled** will block external content will preventing the unwanted gathering of user information. This option was renamed in Office 2007, and its name does not seem to accurately reflect its behavior.

Settings: ..\Microsoft Office Outlook 2007\Security\Automatic Picture Download Settings

Group Policy Object	Recommended State	Version	Level	Scorability
Display pictures and external content in HTML e-mail	Disabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Options\Mail 3. Ensure that the BlockExtContent DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Automatic Picture Download Settings 3. Double-Click Display pictures and external content in HTML e-mail. 4. Select Enabled, click OK.

Additional References
CCE-1133-8

1.2.11.2. Whitelisted Automatic Download of External Content: Level II

Description
The **Automatically download content for e-mail from people in Safe Senders and Safe Recipients Lists** option determines if Outlook automatically downloads and displays external content, such as a web beacon, in HTML e-mail if the Sender or Recipient addresses are within a specified list.

Rationale
Malicious e-mail Senders can send HTML e-mail messages with embedded Web beacons. If a User views a malicious e-mail with an embedded web beacon, it may provide confirmation to the Sender that the Recipient's e-mail address is legitimate. Setting this option to **Disabled** will block external content will prevent the unwanted gathering of user information.

Settings: ..\Microsoft Office Outlook 2007\Security\Automatic Picture Download Settings

Group Policy Object	Recommended State	Version	Level	Scorability
Automatically download content for e-mail from people in Safe Senders and Safe Recipients Lists	Disabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Options\Mail 3. Ensure that the UnblockSpecificSenders DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Automatic Picture Download Settings 3. Double-Click Automatically download content for e-mail from people in Safe Senders and Safe Recipients Lists. 4. Select Disabled, click OK.

Additional References
CCE-725-2

1.2.11.3. Safe Zone Automatic Download of External Content: Level II

Description
The **Do not permit download of content from safe zones** option determines if Outlook will automatically download content from safe zones when displaying messages.

Rationale
Malicious e-mail Senders can send HTML e-mail messages with embedded Web beacons. Viewing an e-mail message that contains a Web beacon provides confirmation that the Recipient's e-mail address is valid, which leaves the Recipient vulnerable to additional spam and harmful e-mail. This option was renamed in Office 2007, and its name does not seem to accurately reflect its behavior.

Settings: ..\Microsoft Office Outlook 2007\Security\Automatic Picture Download Settings

Group Policy Object	Recommended State	Version	Level	Scorability
Do not permit download of content from safe zones	Disabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Options\Mail 3. Ensure that the UnblockSafeZone DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Automatic Picture Download Settings 3. Double-Click Do not permit download of content from safe zones. 4. Select Disabled, click OK.

Additional References
CCE-1347-4

1.2.11.4. Trusted Zone Automatic Download of External Content: Level II

Description
The **Block Trusted Zones** option determines whether Outlook automatically downloads content from trusted zones when displaying messages.

Rationale
Malicious e-mail Senders can send HTML e-mail messages with embedded Web beacons. If a

User views a malicious e-mail with an embedded web beacon, it may provide confirmation to the Sender that the Recipient's e-mail address is legitimate. Setting this option to **Enabled** will not automatically download content for sites in Trusted Zones.

Settings: ..\Microsoft Office Outlook 2007\Security\Automatic Picture Download Settings				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Block Trusted Zones	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Options\Mail 3. Ensure that the TrustedZone DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Automatic Picture Download Settings 3. Double-Click Block Trusted Zones. 4. Select Enabled, click OK.

Additional References
CCE-1475-3

1.2.11.5. Automatic Picture Download for Internet Safe Zones Level I

Description
This option determines whether Outlook automatically downloads content from the Internet when displaying messages.

Rationale
Malicious e-mail Senders can send HTML e-mail messages with embedded Web beacons. Viewing an e-mail message that contains a Web beacon provides confirmation that the Recipient's e-mail address is valid, which leaves the Recipient vulnerable to additional spam and harmful e-mail.

Settings: ..\Microsoft Office Outlook 2007\Security\Automatic Picture Download Settings				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Include Internet in Safe Zones for Automatic Picture Download	Disabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Options\Mail 3. Ensure that the Internet DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Automatic Picture Download Settings 3. Double-Click Include Internet in Safe Zones for Automatic Picture Download. 4. Select Disabled, click OK.

Additional References
CCE-1497-7

1.2.11.6. Automatic Picture Download for Internet Safe Zones Level II

Description
This option determines whether Outlook automatically downloads content from Intranet when displaying messages.

Rationale
Malicious e-mail Senders can send HTML e-mail messages with embedded Web beacons. Viewing an e-mail message that contains a Web beacon provides confirmation that the Recipient's e-mail address is valid, which leaves the Recipient vulnerable to additional spam and harmful e-mail

Settings: ..\Microsoft Office Outlook 2007\Security\Automatic Picture Download Settings

Group Policy Object	Recommended State	Version	Level	Scorability
Include Intranet in Safe Zones for Automatic Picture Download	Disabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Options\Mail 3. Ensure that the Intranet DWORD exists and is set to 0.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
   Microsoft Office Outlook 2007\Security\Automatic Picture Download Settings
3. Double-Click Include Intranet in Safe Zones for Automatic Picture Download.
4. Select Disabled, click OK.

Additional References
CCE-1501-6

1.2.12. Macro / Script Security

1.2.12.1. Allow scripts in one-off Outlook form: Level I

Description
The **Allow scripts in one-off Outlook forms** option determines whether Outlook forms run scripts forms in which the script and layout are contained within the message.

Rationale
Setting this option to **Disabled** protects against the execution of potentially malicious code when Outlook forms are embedded in messages.

Settings: ..\Microsoft Office Outlook 2007\Security\Security Form Settings\Custom Form Security

Group Policy Object	Recommended State	Version	Level	Scorability
Allow scripts in one-off Outlook forms	Disabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the EnableOneOffFormScripts DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Security Form Settings\Custom Form Security 3. Double-Click Allow scripts in one-off Outlook forms. 4. Select Disabled, click OK.

Additional References

CCE-1595-8

1.2.12.2. Macro Security Settings: Level I

Description
The **Security setting for macros** option determines Outlook's macro security level.

Rationale
Macros that are not signed by a trusted publisher can originate from malicious Users attempting to gain code execution on a User's machine. Setting this option to **Enabled** will automatically and silently disable unsigned macros. It will also warn Users when signed macros are about to be executed.

Settings: ..\Microsoft Office Outlook 2007\Security\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Security setting for macros	Enabled Warn for signed disable unsigned	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the Level DWORD exists and is set to 3.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Trust Center 3. Double-Click Security setting for macros. 4. Select Enabled, select Warn for signed disable unsigned, and click OK.

Additional References
CCE-1030-6

1.2.12.3. Macro Security Settings: Level II

Description
The **Security setting for macros** option determines Outlook's macro security level.

Rationale
Setting this option to **Never warn disable all** reduces the ability of an attacker to use macros to gain code execution by only permitting signed macros from an entity on a Trusted

Publisher list to run on a User's system.

Settings: ..\Microsoft Office Outlook 2007\Security\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Security setting for macros	Enabled Never warn disable all	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the Level DWORD exists and is set to 4.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Trust Center 3. Double-Click Security setting for macros. 4. Select Enabled, select Never warn disable all, click OK.

Additional References
CCE-1030-6

1.2.12.4. Security Settings for Macros, Add-Ins and SmartTags: Level II

Description
The **Apply macro security settings to macros, add-ins, and SmartTags** option determines how Outlook applies the macro security settings COM add-ins and smart tags.

Rationale
Malicious code may potentially exist in add-ins and SmartTags. Setting this option to **Enabled** will apply macro security settings macros, add-ins and SmartTags.

Settings: ..\Microsoft Office Outlook 2007\Security\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Apply macro security settings to macros, add-ins, and SmartTags	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security

3. Ensure that the DontTrustInstalledFiles DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Trust Center 3. Double-Click Apply macro security settings to macros add-ins and SmartTags. 4. Select Enabled, click OK.

Additional References
CCE-1462-1

1.2.13. Hyperlink Security

1.2.13.1. Links in E-Mail Messages

Description
The **Enable links in e-mail messages** option determines whether hyperlinks are created in e-mails suspected containing phishing messages.

Rationale
Setting this option to **Disabled** will force Outlook to disable all links in alleged phishing messages.

Settings: ..\Microsoft Office Outlook 2007\Security\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Enable links in e-mail messages	Disabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Options\Mail 3. Ensure that the JunkMailEnableLinks DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Trust Center 3. Double-Click Enable links in e-mail messages. 4. Select Disabled, click OK.

Additional References
CCE-1052-0

1.2.14. Calendar Security

1.2.14.1. Publishing to Office Online: Level II

Description
The **Prevent publishing to Office Online** option determines whether Users have the ability to publish calendars to Office Online.

Rationale
Setting this option to **Enabled** will uphold an organization's policy for restricting the use of external resources.

Settings: ..\Microsoft Office Outlook 2007\Tools | Options...\Preferences\Calendar Options\Microsoft Office Online Sharing Service				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Prevent publishing to Office Online	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Options\PubCal 3. Ensure that the DisableOfficeOnline DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Tools | Options...\Preferences\Calendar Options\Microsoft Office Online Sharing Service 3. Double-Click Prevent publishing to Office Online. 4. Select Enabled, click OK.

Additional References
CCE-1478-7

1.2.14.2. Publishing to DAV Server: Level II

Description
This option determines whether a User can publish his or her calendar to a WebDAV server.

Rationale
WebDAV does not provide sufficiently configurable options for restricting access to published calendars and can allow unauthorized people from accessing sensitive information.

Settings: ..\Microsoft Office Outlook 2007\Tools | Options...\Preferences\Calendar Options\Microsoft Office Online Sharing Service				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Prevent publishing to a DAV server	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Options\PubCal 3. Ensure that the DisableDav DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Tools | Options...\Preferences\Calendar Options\Microsoft Office Online Sharing Service 3. Double-Click Prevent publishing to a DAV server. 4. Select Enabled, click OK.

Additional References
CCE-1368-0

1.2.14.3. Restrict Level of Calendar Details: Level I

Description
The **Restrict level of calendar details Users can publish** option determines the level of calendar details Users can publish to Office Online.

Rationale
Setting this option to **All options are available** will protect against an information leak by publishing excessive details to a public forum.

Settings: ..\Microsoft Office Outlook 2007\Tools | Options...\Preferences\Calendar Options\Microsoft Office Online Sharing Service				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**

Restrict level of calendar details Users can publish	Enabled All options are available	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Options\PubCal 3. Ensure that the PublishCalendarDetailsPolicy DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Tools | Options...\Preferences\Calendar Options\Microsoft Office Online Sharing Service 3. Double-Click Restrict level of calendar details Users can publish. 4. Select Enabled, select All options are available, click OK.

Additional References
CCE-1641-0

1.2.14.4. Restrict Level of Calendar Details: Level II

Description
The **Restrict level of calendar details Users can publish** option determines the level of calendar details Users can publish to Office Online.

Rationale
Setting this option to **Disables 'Full details' and 'Limited details'** will protect against an information leak by publishing excessive details to a public forum.

Settings: ..\Microsoft Office Outlook 2007\Tools | Options...\Preferences\Calendar Options\Microsoft Office Online Sharing Service

Group Policy Object	Recommended State	Version	Level	Scorability
Restrict level of calendar details Users can publish	Enabled Disables 'Full details' and 'Limited details'	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select:

HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Options\PubCal
3. Ensure that the PublishCalendarDetailsPolicy DWORD exists and is set to 4000.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
   Microsoft Office Outlook 2007\Tools | Options...\Preferences\Calendar Options\Microsoft Office Online Sharing Service
3. Double-Click Restrict level of calendar details Users can publish.
4. Select Enabled, select Disables 'Full details' and 'Limited details', click OK.

Additional References

CCE-1641-0

1.2.14.5. Access to Publish Calendars: Level II

Description

The **Access to published calendars** option determines whether a User can publish to calendars on Office Online or third-party WebDAV servers.

Rationale

Setting this option to **Enabled** will uphold an organization's policy for restricting the use of external resources.

Settings: ..\Microsoft Office Outlook 2007\Tools | Options...\Preferences\Calendar Options\Microsoft Office Online Sharing Service

Group Policy Object	Recommended State	Version	Level	Scorability
Access to published calendars	Enabled	2007	II	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:

HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Options\PubCal
3. Ensure that the RestrictedAccessOnly DWORD exists and is set to 1.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
   Microsoft Office Outlook 2007\Tools | Options...\Preferences\Calendar

Options\Microsoft Office Online Sharing Service 3. Double-Click Access to published calendars. 4. Select Enabled, click OK.

Additional References
CCE-1266-6

1.2.14.6. Restrict Upload Method: Level II

Description
The **Restrict upload method** option determines if Outlook can automatically upload calendar updates to Office Online.

Rationale
Setting this option to **Enabled** will uphold an organization's policy for restricting the use of external resources.

Settings: ..\Microsoft Office Outlook 2007\Tools | Options...\Preferences\Calendar Options\Microsoft Office Online Sharing Service				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Restrict upload method	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Options\PubCal 3. Ensure that the SingleUploadOnly DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Tools | Options...\Preferences\Calendar Options\Microsoft Office Online Sharing Service 3. Double-Click Restrict upload method. 4. Select Enabled, click OK.

Additional References
CCE-1399-5

1.2.14.7. Do Not Include Internet Calendar Integration in Outlook: Level II

Description

The **Do not include Internet Calendar integration in Outlook** option determines if a User has the ability publish or subscribe to an Internet calendar.

Rationale
Setting this option to **Enabled** will reduce attack surface and uphold an organization's policy for restricting the use of external resources.

Settings: ..\Microsoft Office Outlook 2007\Tools | Account Settings\Internet Calendars				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Do not include Internet Calendar integration in Outlook	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Options\WebCal 3. Ensure that the Disable DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Tools | Account Settings\Internet Calendars 3. Double-Click Do not include Internet Calendar integration in Outlook. 4. Select Enabled, click OK.

Additional References
CCE-1461-3

1.2.15. Mail Format Security

1.2.15.1. Read E-Mail as Plain Text: Level II

Description
The **Read e-mail as plain text** option determines whether Outlook renders plain text format for reading messages.

Rationale
Setting this option to **Enabled** reduces the attack surface area of the Office system.

Settings: ..\Microsoft Office Outlook 2007\Tools | Options...\Preferences\E-mail Options

Group Policy Object	Recommended State	Version	Level	Scorability
Read e-mail as plain text	Enabled	2007	II	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Options\Mail
3. Ensure that the ReadAsPlain DWORD exists and is set to 1.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
   Microsoft Office Outlook 2007\Tools | Options...\Preferences\E-mail Options
3. Double-Click Read e-mail as plain text.
4. Select Enabled, click OK.

Additional References

CCE-791-4

1.2.15.2. Message Format: Level II

Description

The **Set message format** option determines the default message format in Outlook.

Rationale

By enabling this option to **Plain Text**, Outlook edits e-mail messages in Plain Text by default, reducing the surface attack area.

Settings: ..\Microsoft Office Outlook 2007\Tools | Options...\Mail Format\Internet Formatting\Message Format

Group Policy Object	Recommended State	Version	Level	Scorability
Set message format	Enabled Plain Text	2007	II	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Options\Mail
3. Ensure that the EditorPreference DWORD exists and is set to 10001.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
      Microsoft Office Outlook 2007\Tools | Options...\Mail Format\Internet Formatting\Message Format
3. Double-Click Set message format.
4. Select Enabled, select Plain Text, and click OK.

Additional References
CCE-1526-3

1.2.16. RSS Feed Security

1.2.16.1. Turn Off RSS: Level II

Description
The **Turn off RSS feature** option determines if RSS is enabled in Outlook.

Rationale
Setting this option to **Enabled** reduces the attack surface area of Outlook.

Settings: ..\Microsoft Office Outlook 2007\Tools | Account Settings\RSS Feeds				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Turn off RSS feature	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Options\RSS 3. Ensure that the Disable DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Tools | Account Settings\RSS Feeds 3. Double-Click Turn off RSS feature. 4. Select Enabled, click OK.

Additional References
CCE-1620-4

1.2.17. Miscellaneous

1.2.17.1. Junk E-Mail Protection: Level I

Description
The **Junk E-mail protection level** option controls Outlook's level of junk e-mail filtering.

Rationale
Setting this option to **Low** moves the most obvious spam messages to a User's Junk E-mail folder. Spam may still remain in the User's inbox.

Settings: ..\Microsoft Office Outlook 2007\Tools | Options...\Preferences\Junk E-mail				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Junk E-mail protection level	Enabled Low	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Options\Mail 3. Ensure that the JunkMailProtection DWORD exists and is set to 6.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Tools | Options...\Preferences\Junk E-mail 3. Double-Click Junk E-mail protection level. 4. Select Enabled, select Low, and click OK.

Additional References
CCE-1588-3

1.2.17.2. Junk E-Mail Protection: Level II

Description
The **Junk E-mail protection level** option controls Outlook's level of junk e-mail filtering.

Rationale
Setting this option to **High** may classify legitimate messages as junk mail, however moves the majority of spam messages to a User's Junk E-mail folder.

Settings: ..\Microsoft Office Outlook 2007\Tools | Options...\Preferences\Junk E-mail				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Junk E-mail protection level	Enabled High	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Options\Mail 3. Ensure that the JunkMailProtection DWORD exists and is set to 3.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Tools | Options...\Preferences\Junk E-mail 3. Double-Click Junk E-mail protection level (No Protection Low High Trusted Lists Only). 4. Select Enabled, select High, and click OK.

Additional References
CCE-1588-3

1.2.17.3. Disable Adding E-mail Recipients to User's Safe Senders List: Level I

Description
This setting controls whether Outlook automatically adds a Recipient's E-mail address is to the User's Safe Senders List.

Rationale
Disabling the **Add e-mail Recipients to Users' Safe Senders Lists** option protects against messages from mailing lists purposefully sent to a User's Junk Mail folder being inadvertently sent to an Inbox if the User sends a request to the mailing list asking to be removed.

Settings: ..\Microsoft Office Outlook 2007\Tools | Options...\Preferences\Junk E-mail				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Add e-mail Recipients to Users' Safe Senders Lists	Disabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Options\Mail 3. Ensure that the JunkMailTrustOutgoingRecipients DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Tools | Options...\Preferences\Junk E-mail 3. Double-Click Add e-mail Recipients to Users' Safe Senders Lists. 4. Select Disabled, click OK.

Additional References
CCE-1130-4

1.2.17.4. Dial-Up Options: Level I

Description
The **Dial-up options** setting determines how Outlook connects to dial-up accounts.

Rationale
The **Warn before switching an existing dial-up connection** prevents a User inadvertently connecting to a malicious dial-up connection by warning a User before switching to an alternative connection.

Settings: ..\Microsoft Office Outlook 2007\Tools | Options...\Mail Setup				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Dial-up options	Enabled Warn before switching an existing dial-up connection	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Options 3. Ensure that the Mail DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Tools | Options...\Mail Setup 3. Double-Click Dial-up options. 4. Select Enabled, select Warn before switching an existing dial-up connection, click OK.

Additional References
CCE-1599-0

1.2.17.5. Do Not Allow Creating/Replying/Forwarding Signatures: Level II

Description
The **Do not allow creating replying or forwarding signatures for e-mail messages** option determines if Outlook creates and use e-mail signatures.

Rationale
Setting this option to **Disabled** will verify authenticity of the E-mail Sender.

Settings: ..\Microsoft Office Outlook 2007\Tools | Options...\Mail Format				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Do not allow creating replying or forwarding signatures for e-mail messages	Disabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\MailSettings 3. Ensure that the DisableSignatures DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Tools | Options...\Mail Format 3. Double-Click Do not allow creating replying or forwarding signatures for e-mail messages. 4. Select Disabled, click OK.

Additional References

1.2.17.6. Enable the Person Names Smart Tag Options: Level II

Description
The **Turn off Enable the Person Names Smart Tag** option controls whether Person Names smart tags appear in Outlook.

Rationale
Setting this option to **Enabled** ensures that a User cannot utilize the “Person Names” smart tag, which recognizes names of people in e-mail messages and marks them with smart tag

indicators. These indicators can be selected be used to retrieve data about the person from Active Directory.

Settings: ..\Microsoft Office Outlook 2007\Tools | Options...\Other\Person Names				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Turn off Enable the Person Names Smart Tag option	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\IM 3. Ensure that the Enabled DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Tools | Options...\Other\Person Names 3. Double-Click Turn off Enable the Person Names Smart Tag option. 4. Select Enabled, click OK.

Additional References
CCE-1648-5

1.2.17.7. Outlook Security Mode: Level I

Description
The **Outlook Security Mode** option determines which security settings are enforced by Outlook.

Rationale
Outlook ignores Group Policy settings by default and allows a User to determine their own settings which could lead to the insecure configuration of Outlook. Setting this option to **Enabled** will force Outlook to use Group Policy security settings.

Settings: ..\Microsoft Office Outlook 2007\Security\Security Form Settings				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Outlook Security Mode	Enabled Use Outlook Security Group Policy	2007	I	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security
3. Ensure that the AdminSecurityMode DWORD exists and is set to 3.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
   Microsoft Office Outlook 2007\Security\Security Form Settings
3. Double-Click Outlook Security Mode.
4. Select Enabled, select Use Outlook Security Group Policy, and click OK.

Additional References

CCE-1516-4

1.2.17.8. Retrieving CRLs: Level I

Description

The **Retrieving CRLs** option controls how Outlook verifies the validity of certificates with the Certificate Revocation Lists.

Rationale

Outlook may trust a revoked certificate, potentially putting a User's computer and data at risk. Setting this option to Enabled will enforce that the CRL is updated regularly.

Settings: ..\Microsoft Office Outlook 2007\Security\Cryptography\Signature Status dialog box

Group Policy Object	Recommended State	Version	Level	Scorability
Retrieving CRLs	Enabled When online always retrieve the CRL	2007	I	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security
3. Ensure that the UseCRLChasing DWORD exists and is set to 1.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\

Microsoft Office Outlook 2007\Security\Cryptography\Signature Status dialog box 3. Double-Click Retrieving CRLs. 4. Select Enabled, select When online always retrieve the CRL, click OK.

Additional References
CCE-395-4

1.2.17.9. Missing CRLs: Level II

Description
The **Missing CRLs** setting controls whether Outlook produces an error or a warning for a missing Certificate Revocation List.

Rationale
Setting this option to Enabled will prevent Outlook Users from using certificates when the appropriate CRL is not available to verify them. This could potentially cause some usability issues.

Settings: ..\Microsoft Office Outlook 2007\Security\Cryptography\Signature Status dialog box

Group Policy Object	Recommended State	Version	Level	Scorability
Missing CRLs	Enabled error	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the SigStatusNoCRL DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Cryptography\Signature Status dialog box 3. Double-Click Missing CRLs. 4. Select Enabled, select error, click OK.

Additional References
CCE-1662-6

1.2.17.10. Promote Level 2 Errors as Errors: Level II

Description

The **Promote Level 2 errors as errors, not warnings** option determines if Outlook promotes level 2 cryptographic errors as errors or warnings.

Rationale
Setting this option to **Disabled** will force Outlook to promote these Level 2 errors as errors, preventing the User from continuing with the certificate.

Settings: ..\Microsoft Office Outlook 2007\Security\Cryptography\Signature Status dialog box				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Promote Level 2 errors as errors, not warnings	Disabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the PromoteErrorsAsWarnings DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Cryptography\Signature Status dialog box 3. Double-Click Promote Level 2 errors as errors not warnings. 4. Select Disabled, click OK.

Additional References
CCE-943-1

1.2.17.11. User Entries to Server List: level II

Description
The **Disable User entries to server list** option controls whether Outlook Users have the ability to add entries to the list of SharePoint servers when establishing a meeting workspace.

Rationale
Setting this option to **Publish default Deny others** will disable the ability for Users to add entries to a server list. If Users are allowed to add entries to the list of SharePoint servers, a malicious User could bait meeting invitees to visit a maliciously configured SharePoint server.

Settings: ..\Microsoft Office Outlook 2007\Meeting Workspace

Group Policy Object	Recommended State	Version	Level	Scorability
Disable User entries to server list	Enabled Publish default Deny others	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Meetings\Profile 3. Ensure that the ServerUI DWORD exists and is set to 4.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Meeting Workspace 3. Double-Click Disable User entries to server list. 4. Select Enabled, select Publish default Deny others, click OK.

Additional References
CCE-1041-3

1.3. Excel

1.3.1. Macro Security

1.3.1.1. Scan Encrypted Macros for Viruses: Level I

Description
The **Determine whether to force encrypted macros to be scanned in Microsoft Excel Open XML workbooks** option determines if Excel scans encrypted macros with anti-virus software before opening Open XML workbooks.

Rationale
Setting this option to **Disabled** will scan encrypted macros for viruses before loading them. To avoid bypassing IDS and IPS systems, scanning the macros right before execution will compare signatures of known malicious against the unencrypted macro and halt execution if it matches.

Settings: ..\Microsoft Office Excel 2007\Excel Options\Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**

Determine whether to force encrypted macros to be scanned in Microsoft Excel Open XML workbooks	Disabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Excel\Security 3. Ensure that the ExcelBypassEncryptedMacroScan DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Excel 2007\Excel Options\Security 3. Double-Click Determine whether to force encrypted macros to be scanned in Microsoft Excel Open XML workbooks. 4. Select Disabled, click OK.

Additional References
CCE-1308-6

1.3.1.2. VBA Macro Warnings: Level I

Description
The **VBA Macro Warning Settings** option determines whether Office applications notify the User when VBA macros exist in a document.

Rationale
By default, Users can enable any macro manually through the Trust Bar. Setting this option to **Trust Bar warning for all macros** prevents Users from enabling all macros.

Settings: ..\Microsoft Office Excel 2007\Excel Options\Security\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
VBA Macro Warning Settings	Enabled Trust Bar warning for all macros	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Excel\Security 3. Ensure that the VBAWarnings DWORD exists and is set to 2.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Excel 2007\Excel Options\Security\Trust Center 3. Double-Click VBA Macro Warning Settings. 4. Select Enabled, select Trust Bar warning for all macros, and click OK.

Additional References
CCE-649-4

1.3.1.3. VBA Macro Warnings: Level II

Description
The **VBA Macro Warning Settings** option determines whether Office applications notify the User when VBA macros exist in a document.

Rationale
By default, Users can enable any macro manually through the Trust Bar. A malicious User may use an unsigned macro in an attempt to gain code execution on a User's machine. Setting this option to **Trust Bar warning for digitally signed macros only (unsigned macros will be disabled)** limits execution to signed macros, reducing the attack surface area of this application.

Settings: ..\Microsoft Office Excel 2007\Excel Options\Security\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
VBA Macro Warning Settings	Enabled Trust Bar warning for digitally signed macros only (unsigned macros will be disabled)	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Excel\Security 3. Ensure that the VBAWarnings DWORD exists and is set to 3.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\

Microsoft Office Excel 2007\Excel Options\Security\Trust Center 3. Double-Click VBA Macro Warning Settings. 4. Select Enabled, select Trust Bar warning for digitally signed macros only (unsigned macros will be disabled), click OK.

Additional References
CCE-649-4

1.3.1.4. Trust Access to Visual Basic Project: Level I

Description
The **Trust access to Visual Basic Project** option determines VSTO can access the VBA project system.

Rationale
Setting this option to **Disabled** prevents Users from allowing Excel documents which contain macros to access core Visual Basic objects, methods, and properties.

Settings: ..\Microsoft Office Excel 2007\Excel Options\Security\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Trust access to Visual Basic Project	Disabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Excel\Security 3. Ensure that the AccessVBOM DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Excel 2007\Excel Options\Security\Trust Center 3. Double-Click Trust access to Visual Basic Project. 4. Select Disabled, click OK.

Additional References
CCE-862-3

1.3.2. File Conversion, Opening and Saving Security

1.3.2.1. AutoRepublish: Level II

Description

The **Disable AutoRepublish** option determines whether Users are allowed to use the Auto Republish feature in Excel.

Rationale
By auto-republishing data on every save, Users may unintentionally publish false or sensitive data to the Internet. Enabling this option restricts Users from automatically publishing data to the Internet.

Settings: ..\Microsoft Office Excel 2007\Excel Options\Save				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable AutoRepublish	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Excel\Options 3. Ensure that the DisableAutoRepublish DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Excel 2007\Excel Options\Save 3. Double-Click Disable AutoRepublish. 4. Select Enabled, click OK.

Additional References
CCE-1295-5

1.3.2.2. Enable AutoRepublish Warnings: Level I

Description
The **AutoRepublish Warning Alert** option determines whether Users are notified when Excel auto-republishes content.

Rationale
By auto-republishing data on every save, Users may inadvertently publish false or sensitive data to the Internet. Enabling this option to **Always show the alert** before publishing presents a warning to Users on every save that they are publishing to the Internet. This provides the User the decision of whether or not to publish to the Internet when saving.

Settings: ..\Microsoft Office Excel 2007\Excel Options\Save				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**

AutoRepublish Warning Alert	Enabled Always show the alert before publishing	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Excel\Options 3. Ensure that the DisableAutoRepublishWarning DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Excel 2007\Excel Options\Save 3. Double-Click AutoRepublish Warning Alert. 4. Select Enabled, select Always show the alert before publishing, and click OK.

Additional References
CCE-1334-2

1.3.2.3. Do Not Show Data Extraction Options: Level II

Description
The **Do not show data extraction options when opening corrupt workbooks** option determines whether Excel will present the User with a list of data extraction options before beginning an Open and Repair operation.

Rationale
Enabling this option to **Do not show data extraction options when opening corrupt workbooks** reduces attack surface by forcing Excel to open files using the Safe Load process and does not prompt the User to determine action.

Settings: ..\Microsoft Office Excel 2007\Data Recovery				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Do not show data extraction options when opening corrupt workbooks	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Excel\Options 3. Ensure that the ExtractDataDisableUI DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Excel 2007\Data Recovery 3. Double-Click Do not show data extraction options when opening corrupt workbooks. 4. Select Enabled, click OK.

Additional References
CCE-1094-2

1.3.2.4. File extension and type mismatch: Level I

Description
The **Force file extension to match file type** setting determines how Excel handles files whose type does not match their file extension.

Rationale
A malicious User can bypass Intrusion Detection and Intrusion Prevention systems by changing file extensions may potentially cause Users to open files crafted to exploit Excel flaws. To preserve usability, setting this option to **Allow different but warn** allows Users to manually load files with a different extension.

Settings: ..\Microsoft Office Excel 2007\Excel Options\Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Force file extension to match file type	Enabled Allow different but warn	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Excel\Security 3. Ensure that the ExtensionHardening DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Excel 2007\Excel Options\Security 3. Double-Click Force file extension to match file type. 4. Select Enabled, select Allow different but warn, click OK.

Additional References
CCE-616-3

1.3.2.5. File extension and type mismatch: Level II

Description
The **Force file extension to match file type** setting determines how Excel handles files whose type does not match their file extension.

Rationale
A malicious User can bypass Intrusion Detection and Intrusion Prevention systems by changing file extensions may potentially cause Users to open files crafted to exploit Excel flaws. Setting this option to **Always match file type** will only load files with matching extensions and type.

Settings: ..\Microsoft Office Excel 2007\Excel Options\Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Force file extension to match file type	Enabled Always match file type	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Excel\Security 3. Ensure that the ExtensionHardening DWORD exists and is set to 2.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Excel 2007\Excel Options\Security 3. Double-Click Force file extension to match file type. 4. Select Enabled, select Always match file type, and click OK.

Additional References
CCE-616-3

1.3.2.6. Block Opening Pre-Release Versions of Excel 2007 Files: Level II

Description
The **Block opening of files created by pre-release versions of Excel 2007** option determines if Excel can open prior versions of Excel files.

Rationale

Setting this option to **Enabled** lessens the attack surface area of the application.

Settings: ..\Microsoft Office Excel 2007\Block file formats\Open				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Block opening of files created by pre-release versions of Excel 2007	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Excel\Security\FileOpenBlock 3. Ensure that the Excel12BetaFiles DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Excel 2007\Block file formats\Open 3. Double-Click Block opening of files created by pre-release versions of Excel 2007. 4. Select Enabled, click OK.

Additional References
CCE-1331-8

1.3.2.7. Block Opening of Binary12 File Types: Level II

Description
The **Block opening of Binary12 file types** option determines whether Excel can open Binary12 files.

Rationale
Setting this option to **Enabled** lessens the attack surface area of the application.

Settings: ..\Microsoft Office Excel 2007\Block file formats\Open				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Block opening of Binary12 file types	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select:

HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Excel\Security\FileOpenBlock
3. Ensure that the Binary12Files DWORD exists and is set to 1.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
   Microsoft Office Excel 2007\Block file formats\Open
3. Double-Click Block opening of Binary 12 file types.
4. Select Enabled, click OK.

Additional References

CCE-1490-2

1.3.2.8. Block Opening of HTML and XMLSS File Types: Level II

Description

The **Block opening of HTML and XMLSS files types** option determines whether Excel can open HTML and XMLSS files.

Rationale

Setting this option to **Enabled** lessens the attack surface area of the application.

Settings: ..\Microsoft Office Excel 2007\Block file formats\Open

Group Policy Object	Recommended State	Version	Level	Scorability
Block opening of HTML and XMLSS files types	Enabled	2007	II	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:

HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Excel\Security\FileOpenBlock
3. Ensure that the HtmlandXmlssFiles DWORD exists and is set to 1.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
   Microsoft Office Excel 2007\Block file formats\Open
3. Double-Click Block opening of HTML and Xmlss files types.
4. Select Enabled, click OK.

Additional References
CCE-1543-8

1.3.2.9. Block Opening of XML File Types: Level II

Description
The **Block opening of XML file types** option determines if Excel can open XML files.

Rationale
Setting this to **Enabled** option lessens the attack surface area of the application.

Settings: ..\Microsoft Office Excel 2007\Block file formats\Open				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Block opening of XML file types	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Excel\Security\FileOpenBlock 3. Ensure that the XmlFiles DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Excel 2007\Block file formats\Open 3. Double-Click Block opening of XML file types. 4. Select Enabled, click OK.

Additional References
CCE-1195-7

1.3.2.10. Block Opening DIF and SYLK File Types: Level II

Description
The **Block opening of DIF and SYLK file types** option determines if Excel can open DIF and SYLK files.

Rationale
Setting this option to **Enabled** lessens the attack surface area of the application.

Settings: ..\Microsoft Office Excel 2007\Block file formats\Open				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Block opening of DIF and SYLK file types	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Excel\Security\FileOpenBlock 3. Ensure that the DifandSylkFiles DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Excel 2007\Block file formats\Open 3. Double-Click Block opening of DIF and SYLK file types. 4. Select Enabled, click OK.

Additional References
CCE-554-6

1.3.2.11. Block Opening of XLL File Types: Level II

Description
The **Block opening of XLL file type** option determines if Excel can open XLL files.

Rationale
Setting this option to **Enabled** lessens the attack surface area of the application.

Settings: ..\Microsoft Office Excel 2007\Block file formats\Open				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Block opening of XLL file type	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Excel\Security\FileOpenBlock 3. Ensure that the XllFiles DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Excel 2007\Block file formats\Open 3. Double-Click Block opening of Xll file type. 4. Select Enabled, click OK.

Additional References
CCE-1437-3

1.3.2.12. Block Opening of XML Files: Level II

Description
The **Block opening of Open XML file types** option determines if Excel can open Open XML files.

Rationale
Setting this option to **Disabled** will allow Excel to open XML file types because Open XML has built-in security features that make it a safe format for saving.

Settings: ..\Microsoft Office Excel 2007\Block file formats\Open				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Block opening of Open XML file types	Disabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Excel\Security\FileOpenBlock 3. Ensure that the OpenXmlFiles DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Excel 2007\Block file formats\Open 3. Double-Click Block opening of Open XML file types. 4. Select Disabled, click OK.

Additional References
CCE-1468-8

1.3.3. Hidden Text / Meta Data Security

1.3.3.1. Save Data Necessary to Maintain Formulas: Level II

Description
The **Save any additional data necessary to maintain formulas** option determines if Excel saves hidden data when saved as a web page using Office Web Components (OWC) to maintain formulas.

Rationale
Hidden data can expose sensitive information to unauthorized viewers of the saved web page. Setting the state to **Disabled** will prevent Users from inadvertently saving hidden data in workbook pages.

Settings: ..\Microsoft Office Excel 2007\Excel Options\Advanced\Web Options...\General

Group Policy Object	Recommended State	Version	Level	Scorability
Save any additional data necessary to maintain formulas	Disabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Excel\Internet 3. Ensure that the DoNotSaveHiddenData DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Excel 2007\Excel Options\Advanced\Web Options...\General 3. Double-Click Save any additional data necessary to maintain formulas. 4. Select Disabled, click OK.

Additional References
CCE-1277-3

1.3.4. Dynamic Data Exchange

1.3.4.1. Application Communication via DDE: Level II

Description
The **Ignore other applications** option determines whether Excel exchanges data with other applications that use Dynamic Data Exchange (DDE).

Rationale
DDE is often used to link Excel cells with data in other applications, allowing the linked cells to be updated automatically. Data integrity could be compromised in some situations since updating occurs automatically and thereby without User intervention.

Settings: ..\Microsoft Office Excel 2007\Excel Options\Advanced				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Ignore other applications	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Excel\Options\BinaryOptions 3. Ensure that the fDdeEnabled_6_1 DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Excel 2007\Excel Options\Advanced 3. Double-Click Ignore other applications . 4. Select Enabled, click OK.

Additional References
CCE-1471-2

1.3.4.2. Ask to Update Automatic Links: Level II

Description
The **Ask to update automatic links** option determines whether Excel updates links automatically in the background or prompt a User for updates.

Rationale
Setting this option to **Enabled** will protect against the automatic update of links without User interaction which could unintentionally compromise data integrity in a workbook.

Settings: ..\Microsoft Office Excel 2007\Excel Options\Advanced				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Ask to update automatic links	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Excel\Options\BinaryOptions 3. Ensure that the fUpdateExt_78_1 DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Excel 2007\Excel Options\Advanced 3. Double-Click Ask to update automatic links. 4. Select Enabled, click OK.

Additional References
CCE-1119-7

1.3.5. Automatic Download Security

1.3.5.1. Graphics Loading from non-Excel Created Web Pages: Level II

Description
The **Load pictures from Web pages not created in Excel** option forces Excel to not load graphics that were not created in Excel when opening web pages.

Rationale
Disabling this option reduces the attack surface area of Excel by preventing the loading of future vulnerable graphic files.

Settings: ..\Microsoft Office Excel 2007\Excel Options\Advanced\Web Options...\General				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Load pictures from Web pages not created in Excel	Disabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Excel\Internet 3. Ensure that the DoNotLoadPictures DWORD exists and is set to 1.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
   Microsoft Office Excel 2007\Excel Options\Advanced\Web Options…\General
3. Double-Click Load pictures from Web pages not created in Excel.
4. Select Disabled, click OK.

Additional References
CCE-1464-7

1.3.6. Add-In Security

1.3.6.1. Disable all Application Add-Ins: Level II

Description
The **Disable all application add-ins** setting determines if application add-ins are initialized.

Rationale
Application add-ins could potentially be used by a malicious User to gain code execution on a User's box. Setting this option to **Enabled** will disable all application add-ins.

Settings: ..\Microsoft Office Excel 2007\Excel Options\Security\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable all application add-ins	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Excel\Security 3. Ensure that the DisableAllAddins DWORD does not exist.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Excel 2007\Excel Options\Security\Trust Center 3. Double-Click Disable all application add-ins. 4. Select Not Configured, click OK.

Additional References
CCE-1251-8

1.3.6.2. Require Signed Application Add-Ins: Level II

Description
The **Require that application add-ins are signed by Trusted Publisher** option determines if application add-ins must be signed by a Trusted Publisher.

Rationale
A malicious User may use unsigned add-ins to gain code execution on a User's machine. Setting this option to **Enabled** will require that all executed add-ins must be signed by a Trusted Publisher.

Settings: ..\Microsoft Office Excel 2007\Excel Options\Security\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Require that application add-ins are signed by Trusted Publisher	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Excel\Security 3. Ensure that the RequireAddinSig DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Excel 2007\Excel Options\Security\Trust Center 3. Double-Click Require that application add-ins are signed by Trusted Publisher. 4. Select Enabled, click OK.

Additional References
CCE-1524-8

1.3.6.3. TrustBar Notification or Unsigned Add-Ins: Level II

Description
The **Disable Trust Bar Notification for unsigned application add-ins** option determines whether Trust Bar Notifications are displayed when unsigned application add-ins are loaded, or whether they are silently disabled and prevented from executing.

Rationale
A malicious User may use unsigned add-ins to gain code execution on a User's machine. Setting this option to **Enabled** forces Excel to automatically and silently disable unsigned application add-ins.

Settings: ..\Microsoft Office Excel 2007\Excel Options\Security\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable Trust Bar Notification for unsigned application add-ins	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Excel\Security 3. Ensure that the NoTBPromptUnsignedAddin DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Excel 2007\Excel Options\Security\Trust Center 3. Double-Click Disable Trust Bar Notification for unsigned application add-ins. 4. Select Enabled, click OK.

Additional References
CCE-1422-5

1.3.7. Trusted Location Security

1.3.7.1. External Trusted Locations: Level I

Description
The **Allow External Trusted Locations not on the computer** option determines if locations on the network can be used as a Trusted Location.

Rationale
Files loaded into Trusted Locations may be controlled by malicious Users and are not subject to security measures. Setting this option to **Disabled** reduces the attack surface of Excel by not allowing network locations to be regarded as Trusted Locations.

Settings: ..\Microsoft Office Excel 2007\Excel Options\Security\Trust Center\Trusted Locations				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Allow Trusted Locations not on the computer	Disabled	2007	I	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:

HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Excel\Security\Trusted Locations
3. Ensure that the AllowNetworkLocations DWORD exists and is set to 0.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
   Microsoft Office Excel 2007\Excel Options\Security\Trust Center\Trusted Locations
3. Double-Click Allow Trusted Locations not on the computer.
4. Select Disabled, click OK.

Additional References

CCE-1444-9

1.3.7.2. Disable all Trusted Locations: Level II

Description

The **Disable all trusted locations** option determines if Excel disables all Trusted Locations.

Rationale

Files loaded into Trusted Locations may be controlled by malicious Users and are not subject to security measures. Setting this option to **Enabled** reduces the attack surface of Excel by disabling all Trusted Locations.

Settings: ..\Microsoft Office Excel 2007\Excel Options\Security\Trust Center\Trusted Locations

Group Policy Object	Recommended State	Version	Level	Scorability
Disable all trusted locations	Enabled	2007	II	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:

HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Excel\Security\Trusted Locations
3. Ensure that the AllLocationsDisabled DWORD exists and is set to 1.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:

User Configuration\Administrative Templates\
Microsoft Office Excel 2007\Excel Options\Security\Trust Center\Trusted Locations
3. Double-Click Disable all trusted locations.
4. Select Enabled, click OK.

Additional References
CCE-1449-8

1.4. Word

1.4.1. Macro Security

1.4.1.1. Scan Encrypted Macros for Viruses: Level I

Description
The **Determine whether to force encrypted macros to be scanned in Microsoft Word Open XML workbooks** option determines if Word scans encrypted macros with anti-virus software before opening Open XML workbooks.

Rationale
Setting this option to **Enabled** will scan encrypted macros for viruses before loading them. To avoid bypassing IDS and IPS systems, scanning the macros right before execution will compare signatures of known malicious against the unencrypted macro and halt execution if it matches.

Settings: ..\Microsoft Office Word 2007\Word Options\Security\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Determine whether to force encrypted macros to be scanned in Microsoft Word Open XML documents	Enabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Word\Security 3. Ensure that the WordBypassEncryptedMacroScan DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Word 2007\Word Options\Security\Trust Center

3. Double-Click Determine whether to force encrypted macros to be scanned in Microsoft Word Open XML documents. 4. Select Enabled, click OK.

Additional References
CCE-1280-7

1.4.1.2. VBA Macro Warning Settings: Level I

Description
The **VBA Macro Warning Settings** option determines whether Office applications notify the User when VBA macros exist in a document.

Rationale
By default, Users can enable any macro manually through the Trust Bar. Setting this option to **Trust Bar warning for all macros** prevents Users from enabling all macros.

Settings: ..\Microsoft Office Word 2007\Word Options\Security\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
VBA Macro Warning Settings	Enabled Trust Bar warning for all macros	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Word\Security 3. Ensure that the VBAWarnings DWORD exists and is set to 2.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Word 2007\Word Options\Security\Trust Center 3. Double-Click VBA Macro Warning Settings. 4. Select Enabled, select Trust Bar warning for all macros, and click OK.

Additional References
CCE-659-3

1.4.1.3. VBA Macro Warning Settings: Level II

Description
The **VBA Macro Warning Settings** option determines whether Office applications notify the

User when VBA macros exist in a document.

Rationale
By default, Users can enable any macro manually through the Trust Bar. A malicious User may use an unsigned macro in an attempt to gain code execution on a User's machine. Setting this option to **Trust Bar warning for digitally signed macros only (unsigned macros will be disabled)** limits execution to signed macros, reducing the attack surface area of this application.

Settings: ..\Microsoft Office Word 2007\Word Options\Security\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
VBA Macro Warning Settings	Enabled Trust Bar warning for digitally signed macros only (unsigned macros will be disabled)	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Word\Security 3. Ensure that the VBAWarnings DWORD exists and is set to 3.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Word 2007\Word Options\Security\Trust Center 3. Double-Click VBA Macro Warning Settings. 4. Select Enabled, select Trust Bar warning for digitally signed macros only (unsigned macros will be disabled), click OK.

Additional References
CCE-427-5

1.4.1.4. Trust Access to Visual Basic Project: Level I

Description
The **Trust access to Visual Basic Project** option determines whether automation clients such as VSTO can access the VBA project system.

Rationale
Disabling this option prevents Users from allowing potentially malicious macros in Word

documents to access core Visual Basic objects, methods, and properties.

Settings: ..\Microsoft Office Word 2007\Word Options\Security\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Trust access to Visual Basic Project	Disabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Word\Security 3. Ensure that the AccessVBOM DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Word 2007\Word Options\Security\Trust Center 3. Double-Click Trust access to Visual Basic Project. 4. Select Disabled, click OK.

Additional References
CCE-703-9

1.4.2. File Conversion and Opening Security

1.4.2.1. Block Opening of HTML File Types: Level II

Description
The **Block opening of HTML file types** option determines whether Word can open HTML files.

Rationale
Setting this option to **Enabled** will block opening of HTML file types lessens the attack surface area of Word by preventing against the exploitation of future vulnerabilities.

Settings: ..\Microsoft Office Word 2007\Block file formats\Open				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Block opening of HTML file types	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select:

HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Word\Security\FileOpenBlock
3. Ensure that the HtmlFiles DWORD exists and is set to 1.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
   Microsoft Office Word 2007\Block file formats\Open
3. Double-Click Block opening of HTML file types.
4. Select Enabled, click OK.

Additional References

CCE-1644-4

1.4.2.2. Block Opening of RTF File Types: Level II

Description

The **Block opening of RTF file types** option determines whether Word can open RTF files.

Rationale

Enabling this option lessens the attack surface area of the application.

Settings: ..\Microsoft Office Word 2007\Block file formats\Open

Group Policy Object	Recommended State	Version	Level	Scorability
Block opening of RTF file types	Enabled	2007	II	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:

HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Word\Security\FileOpenBlock
3. Ensure that the RtfFiles DWORD exists and is set to 1.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
   Microsoft Office Word 2007\Block file formats\Open
3. Double-Click Block opening of RTF file types.
4. Select Enabled, click OK.

Additional References

CCE-1579-2

1.4.2.3. Block Opening of Converters: Level II

Description
The **Block open Converters** option determines whether Word can open Converters.

Rationale
Enabling this option lessens the attack surface area of the application by preventing Users from opening all types of documents and formats.

Settings: ..\Microsoft Office Word 2007\Block file formats\Open				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Block open Converters	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Word\Security\FileOpenBlock 3. Ensure that the Converters DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Word 2007\Block file formats\Open 3. Double-Click Block open Converters. 4. Select Enabled, click OK.

Additional References
CCE-984-5

1.4.2.4. Block Opening of Internal File Types: Level II

Description
The **Opening of Internal File Type** option determines whether Word can open Word files in pre-release (2003 and earlier) formats.

Rationale
Enabling this option lessens the attack surface area of the application.

Settings: ..\Microsoft Office Word 2007\Block file formats\Open

Group Policy Object	Recommended State	Version	Level	Scorability
Block opening of Internal file types	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Word\Security\FileOpenBlock 3. Ensure that the InternalFiles DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Word 2007\Block file formats\Open 3. Double-Click Block opening of Internal file types. 4. Select Enabled, click OK.

Additional References
CCE-1503-2

1.4.2.5. Block Opening of Files before Version Word 2003: Level II

Description
The **Block opening of files before version** option determines whether Word can open Word files before Word 2003.

Rationale
Setting this option to **Enabled - Word 2003 as saved by Word 2007** lessens the attack surface area of the application by disabling document converters for previous versions of Word.

Settings: ..\Microsoft Office Word 2007\Block file formats\Open				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Block opening of files before version	Enabled Word 2003 as saved by Word 2007	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select:

HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Word\Security\FileOpenBlock 3. Ensure that the FilesBeforeVersion DWORD exists and is set to 112.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Word 2007\Block file formats\Open 3. Double-Click Block opening of files before version. 4. Select Enabled, select Word 2003 as saved by Word 2007, click OK.

Additional References
CCE-1371-4

1.4.2.6. Block Opening of Pre-Release Versions of File Formats: Level II

Description
The **Block opening of pre-release versions of file formats new to Word 2007** option determines if Word with Microsoft Office Compatibility Pack for Word File Formats installed can open formats saved with pre-release versions of Word 2007.

Rationale
Setting this option to **Enabled** reduces the attack surface area of the Office system.

Settings: ..\Microsoft Office Word 2007\Block file formats\Open				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Block opening of pre-release versions of file formats new to Word 2007	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Word\Security\FileOpenBlock 3. Ensure that the Word12BetaFiles DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Word 2007\Block file formats\Open 3. Double-Click Block opening of pre-release versions of file formats new to Word 2007.

4. Select Enabled, click OK.

Additional References
CCE-1549-5

1.4.2.7. Block Opening of Open XML File Types: Level I

Description
The **Block opening of Open XML file types** option determines if Word can open Open XML files.

Rationale
Setting this option to **Disabled** will allow Word to open XML file types because Open XML has built-in security features that make it a safe format for saving.

Settings: ..\Microsoft Office Word 2007\Block file formats\Open				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Block opening of Open XML file types	Enabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Word\Security\FileOpenBlock 3. Ensure that the OpenXmlFiles DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Word 2007\Block file formats\Open 3. Double-Click Block opening of Open XML file types. 4. Select Disabled, click OK.

Additional References
CCE-1504-0

1.4.2.8. Block Opening o Word 2003 XML File Types: Level II

Description
The **Block opening of Word 2003 XML file types** option determines whether Word can open Word 2003 XML files.

Rationale
Setting this option to **Enabled** reduces the attack surface area of the application.

Settings: ..\Microsoft Office Word 2007\Block file formats\Open				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Block opening of Word 2003 XML file types	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Word\Security\FileOpenBlock 3. Ensure that the XmlFiles DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Word 2007\Block file formats\Open 3. Double-Click Block opening of Word 2003 XML file types. 4. Select Enabled, click OK.

Additional References
CCE-958-9

1.4.3. Hidden Text / Meta Data Security

1.4.3.1. Show All Hidden Text: Level II

Description
Setting the **Hidden text** option will force Word to show hidden markup such as comments, revisions, annotations, notes, etc.

Rationale
If a document contains sensitive data that is marked hidden, it may be inadvertently distributed. Setting this option to **Enabled** shows all hidden data on a User's monitor.

Settings: ..\Microsoft Office Word 2007\Word Options\Display				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Hidden text	Enabled	2007	II	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Word\Options\vpref
3. Ensure that the grpfvisi_135_1 DWORD exists and is set to 1.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
   Microsoft Office Word 2007\Word Options\Display
3. Double-Click Hidden text.
4. Select Enabled, click OK.

Additional References

CCE-885-4

1.4.4. Hyperlink Security

1.4.4.1. Update of Automatic Links at Open: Level II

Description

The **Update automatic links at Open** option determines whether Word prompts a User to update automatic links when opening a document, or whether the update occurs automatically in the background.

Rationale

Setting this option to **Disabled** will protect against automatic updating of links without User interaction could inadvertently compromise the integrity of some of the data in the document.

Settings: ..\Microsoft Office Word 2007\Word Options\Advanced

Group Policy Object	Recommended State	Version	Level	Scorability
Update automatic links at Open	Disabled	2007	II	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Word\Options
3. Ensure that the fNoCalcLinksOnOpen_90_1 DWORD exists and is set to 0.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:

User Configuration\Administrative Templates\
Microsoft Office Word 2007\Word Options\Advanced
3. Double-Click Update automatic links at Open.
4. Select Disabled, click OK.

Additional References
CCE-1249-2

1.4.5. Add-In Security

1.4.5.1. Disable all Application Add-Ins: Level I

Description
The **Disable all application add-ins** setting determines if application add-ins are initialized.

Rationale
Application add-ins could potentially be used by a malicious User to gain code execution on a User's box. Setting this option to **Not Configured** will disable all application add-ins.

Settings: ..\Microsoft Office Word 2007\Word Options\Security\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable all application add-ins	Not Configured	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Word\Security 3. Ensure that the DisableAllAddins DWORD does not exist.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Word 2007\Word Options\Security\Trust Center 3. Double-Click Disable all application add-ins. 4. Select Not Configured, click OK.

Additional References
CCE-1681-6

1.4.5.2. Require Signed Application Add-Ins: Level II

Description
The **Require that application add-ins are signed by Trusted Publisher** option determines if

application add-ins must be signed by a Trusted Publisher.

Rationale
A malicious User may use unsigned add-ins to gain code execution on a User's machine. Setting this option to **Enabled** will require that all executed add-ins must be signed by a Trusted Publisher.

Settings: ..\Microsoft Office Word 2007\Word Options\Security\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Require that application add-ins are signed by Trusted Publisher	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Word\Security 3. Ensure that the RequireAddinSig DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Word 2007\Word Options\Security\Trust Center 3. Double-Click Require that application add-ins are signed by Trusted Publisher. 4. Select Enabled, click OK.

Additional References
CCE-1562-8

1.4.5.3. Receive TrustBar Notification for Unsigned Application Add-Ins: Level II

Description
The **Disable Trust Bar Notification for unsigned application add-ins** option determines whether Trust Bar Notifications are displayed when unsigned application add-ins are loaded, or whether they are silently disabled and prevented from executing.

Rationale
A malicious User may use unsigned add-ins to gain code execution on a User's machine. Setting this option to **Enabled** forces Word to automatically and silently disable unsigned application add-ins.

Settings: ..\Microsoft Office Word 2007\Word Options\Security\Trust Center

Group Policy Object	Recommended State	Version	Level	Scorability
Disable Trust Bar Notification for unsigned application add-ins	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Word\Security 3. Ensure that the NoTBPromptUnsignedAddin DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Word 2007\Word Options\Security\Trust Center 3. Double-Click Disable Trust Bar Notification for unsigned application add-ins. 4. Select Enabled, click OK.

Additional References
CCE-1333-4

1.4.6. Trusted Location Security

1.4.6.1. External Trusted Locations: Level I

Description
The **Allow External Trusted Locations** option determines if locations on the network can be used as a Trusted Location.

Rationale
Files loaded into Trusted Locations may be controlled by malicious Users and are not subject to security measures. Setting this option to **Disabled** reduces the attack surface of Word by not allowing network locations to be regarded as Trusted Locations.

Settings: ..\Microsoft Office Word 2007\Word Options\Security\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Allow Trusted Locations not on the computer	Disabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select:

HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Word\Security\Trusted Locations 3. Ensure that the AllowNetworkLocations DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Word 2007\Word Options\Security\Trust Center 3. Double-Click Allow Trusted Locations not on the computer. 4. Select Disabled, click OK.

Additional References
CCE-1355-7

1.4.6.2. Disable all Trusted Locations: Level II

Description
The **Disable all trusted locations** option determines if Word disables all Trusted Locations.

Rationale
Files loaded into Trusted Locations may be controlled by malicious Users and are not subject to security measures. Setting this option to **Enabled** reduces the attack surface by disabling all Trusted Locations.

Settings: ..\Microsoft Office Word 2007\Word Options\Security\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable all trusted locations	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Word\Security\Trusted Locations 3. Ensure that the AllLocationsDisabled DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Word 2007\Word Options\Security\Trust Center 3. Double-Click Disable all trusted locations.

4. Select Enabled, click OK.

Additional References
CCE-782-3

1.5. Power Point

1.5.1. Macro Security

1.5.1.1. Scan Encypted Macros in PowerPoint Open XML: Level I

Description
The **Determine whether to force encrypted macros to be scanned in Microsoft PowerPoint Open XML workbooks** option determines if Word scans encrypted macros with anti-virus software before opening Open XML workbooks.

Rationale
Setting this option to **Enabled** will scan encrypted macros for viruses before loading them. To avoid bypassing IDS and IPS systems, scanning the macros right before execution will compare signatures of known malicious against the unencrypted macro and halt execution if it matches.

Settings: ..\Microsoft Office PowerPoint 2007\PowerPoint Options\Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Determine whether to force encrypted macros to be scanned in Microsoft PowerPoint Open XML presentations	Enabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\PowerPoint\Security 3. Ensure that the PowerPointBypassEncryptedMacroScan DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office PowerPoint 2007\PowerPoint Options\Security 3. Double-Click Determine whether to force encrypted macros to be scanned in Microsoft PowerPoint Open XML presentations. 4. Select Enabled, click OK.

Additional References
CCE-1142-9

1.5.1.2. Receive TrustBar Notifications when Macros Exist: Level I

Description
The **VBA Macro Warning Settings** option determines whether Office applications notify the User when VBA macros exist in a document.

Rationale
By default, Users can enable any macro manually through the Trust Bar. Setting this option to **Trust Bar warning for all macros** prevents Users from enabling all macros.

Settings: ..\Microsoft Office PowerPoint 2007\PowerPoint Options\Security\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
VBA Macro Warning Settings	Enabled Trust Bar warning for all macros	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\PowerPoint\Security 3. Ensure that the VBAWarnings DWORD exists and is set to 2.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office PowerPoint 2007\PowerPoint Options\Security\Trust Center 3. Double-Click VBA Macro Warning Settings. 4. Select Enabled, select Trust Bar warning for all macros, and click OK.

Additional References
CCE-567-8

1.5.1.3. Receive TrustBar Notifications when Signed Macros Exist: Level II

Description
This option determines how Office applications notify the User when VBA macros exist in a document.

Rationale
By default, Users can enable any macro manually through the Trust Bar. A malicious User may use an unsigned macro in an attempt to gain code execution on a User's machine. Setting this option to **Trust Bar warning for digitally signed macros only (unsigned macros will be disabled)** limits execution to signed macros, reducing the attack surface area of this application.

Settings: ..\Microsoft Office PowerPoint 2007\PowerPoint Options\Security\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
VBA Macro Warning Settings	Enabled Trust Bar warning for digitally signed macros only (unsigned macros will be disabled)	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\PowerPoint\Security 3. Ensure that the VBAWarnings DWORD exists and is set to 3.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office PowerPoint 2007\PowerPoint Options\Security\Trust Center 3. Double-Click VBA Macro Warning Settings. 4. Select Enabled, select Trust Bar warning for digitally signed macros only (unsigned macros will be disabled), click OK.

Additional References
CCE-427-5

1.5.1.4. Trust Access to Visual Basic Project: Level I

Description
The **Trust access to Visual Basic Project** option determines whether automation clients such as Visual Studio Tools for Office (VSTO) can access the Visual Basic for Applications (VBA) project system.

Rationale
Setting this option to **Disabled** prevents Users from allowing macros in PowerPoint

documents to access Visual Basic objects, methods, and properties.

Settings: ..\Microsoft Office PowerPoint 2007\PowerPoint Options\Security\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Trust access to Visual Basic Project	Disabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\PowerPoint\Security 3. Ensure that the AccessVBOM DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office PowerPoint 2007\PowerPoint Options\Security\Trust Center 3. Double-Click Trust access to Visual Basic Project. 4. Select Disabled, click OK.

Additional References
CCE-68-7

1.5.2. File Conversion, Opening and Saving Security

1.5.2.1. Block Opening of HTML File Types: Level II

Description
The **Block opening of HTML file types** option determines whether PowerPoint can open HTML files.

Rationale
Setting this option to **Enabled** will block opening of HTML file types lessens the attack surface area of PowerPoint by preventing against the exploitation of future vulnerabilities.

Settings: ..\Microsoft Office PowerPoint 2007\Block file formats\Open				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Block opening of HTML file types	Enabled	2007	II	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\PowerPoint\
   Security\FileOpenBlock
3. Ensure that the HtmlFiles DWORD exists and is set to 1.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
   Microsoft Office PowerPoint 2007\Block file formats\Open
3. Double-Click Block opening of HTML file types.
4. Select Enabled, click OK.

Additional References

CCE-1644-4

1.5.2.2. Block Opening of Outlines: Level II

Description

The **Block opening of Outlines** option determines whether PowerPoint can open Outlines such as .rtf, .txt, .doc, .wpd, .docx, .docm, and .wps files.

Rationale

Enabling this option lessens the attack surface area of the application.

Settings: ..\Microsoft Office PowerPoint 2007\Block file formats\Open

Group Policy Object	Recommended State	Version	Level	Scorability
Block opening of Outlines	Enabled	2007	II	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\PowerPoint\
   Security\FileOpenBlock
3. Ensure that the Outlines DWORD exists and is set to 1.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
   Microsoft Office PowerPoint 2007\Block file formats\Open
3. Double-Click Block opening of Outlines.
4. Select Enabled, click OK.

Additional References
CCE-1194-0

1.5.2.3. Block Opening of Converters: Level II

Description
The **Block Opening of Converters** option determines whether PowerPoint can open Converters, which have the ability to open all document types and formats.

Rationale
Enabling this option lessens the attack surface area of the application by preventing Users from opening all types of documents and formats.

Settings: ..\Microsoft Office PowerPoint 2007\Block file formats\Open				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Block opening of Converters	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\PowerPoint\Security\FileOpenBlock 3. Ensure that the Converters DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\Microsoft Office PowerPoint 2007\Block file formats\Open 3. Double-Click Block opening of Converters. 4. Select Enabled, click OK.

Additional References
CCE-1216-1

1.5.2.4. Block Opening Files Saved with Pre-Release Versions PowerPoint: Level II

Description
The **Block opening of pre-release versions of file formats new to PowerPoint 2007** option determines if PowerPoint with Microsoft Office Compatibility Pack for File Formats installed can open formats saved with pre-release versions of Word 2007.

Rationale
Setting this option to **Enabled** reduces the attack surface area of the Office system.

Settings: ..\Microsoft Office PowerPoint 2007\Block file formats\Open				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Block opening of pre-release versions of file formats new to PowerPoint 2007	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\PowerPoint\Security\FileOpenBlock 3. Ensure that the PowerPoint12BetaFiles DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office PowerPoint 2007\Block file formats\Open 3. Double-Click Block opening of pre-release versions of file formats new to PowerPoint 2007. 4. Select Enabled, click OK.

Additional References
CCE-1594-1

1.5.2.5. Block Opening Open XML Files: Level II

Description
The **Block opening of Open XML file types** option determines if PowerPoint can open Open XML files.

Rationale
Setting this option to **Disabled** will allow PowerPoint to open XML file types because Open XML has built-in security features that make it a safe format for saving.

Settings: ..\Microsoft Office PowerPoint 2007\Block file formats\Open				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Block opening of Open XML files types	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\PowerPoint\Security\FileOpenBlock 3. Ensure that the OpenXmlFiles DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\Microsoft Office PowerPoint 2007\Block file formats\Open 3. Double-Click Block opening of Open XML files types. 4. Select Disabled, click OK.

Additional References
CCE-1701-2

1.5.3. Hidden Text / Meta Data Security

1.5.3.1. Show All Hidden Text: Level II

Description
Setting the **Make hidden markup visible** option will force PowerPoint to show hidden markup such as comments, revisions, annotations, notes, etc.

Rationale
If a document contains sensitive data that is marked hidden, it may be inadvertently distributed. Setting this option to **Enabled** shows all hidden data on a User's monitor.

Settings: ..\Microsoft Office PowerPoint 2007\PowerPoint Options\Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Make hidden markup visible	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\PowerPoint\Security\Trusted Locations\PolLocation20 3. Ensure that the MarkupOpenSave DWORD exists and is set to 1.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
   Microsoft Office PowerPoint 2007\PowerPoint Options\Security
3. Double-Click Make hidden markup visible.
4. Select Enabled, click OK.

Additional References
CCE-1279-9

1.5.4. Automatic Download Security

1.5.4.1. Unblock Automatic Download of Linked Images: Level I

Description
The **Unblock automatic download of linked images** option determines whether a PowerPoint presentation automatically downloads external images.

Rationale
Setting this option to **Disabled** reduces the attack surface area of the PowerPoint.

Settings: ..\Microsoft Office PowerPoint 2007\PowerPoint Options\Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Unblock automatic download of linked images	Disabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\PowerPoint\Security 3. Ensure that the DownloadImages DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office PowerPoint 2007\PowerPoint Options\Security 3. Double-Click Unblock automatic download of linked images. 4. Select Disabled, click OK.

Additional References
CCE-1451-4

1.5.5. Add-In Security

1.5.5.1. Require Signed Application Add-Ins: Level II

Description
The **Require that application add-ins are signed by Trusted Publisher** option determines if application add-ins must be signed by a Trusted Publisher.

Rationale
A malicious User may use unsigned add-ins to gain code execution on a User's machine. Setting this option to **Enabled** will require that all executed add-ins must be signed by a Trusted Publisher.

Settings: ..\Microsoft Office PowerPoint 2007\PowerPoint Options\Security\Trust Center

Group Policy Object	Recommended State	Version	Level	Scorability
Require that application add-ins are signed by Trusted Publisher	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\PowerPoint\Security 3. Ensure that the RequireAddinSig DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office PowerPoint 2007\PowerPoint Options\Security\Trust Center 3. Double-Click Require that application add-ins are signed by Trusted Publisher. 4. Select Enabled, click OK.

Additional References
CCE-1107-2

1.5.5.2. Receive TrustBar Notification for Unsigned Application Add-Ins: Level II

Description
The **Disable Trust Bar Notification for unsigned application add-ins** option determines whether Trust Bar Notifications are displayed when unsigned application add-ins are loaded, or whether they are silently disabled and prevented from executing.

Rationale
A malicious User may use unsigned add-ins to gain code execution on a User's machine. Setting this option to **Enabled** forces PowerPoint to automatically and silently disable unsigned application add-ins.

Settings: ..\Microsoft Office PowerPoint 2007\PowerPoint Options\Security\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable Trust Bar Notification for unsigned application add-ins	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\PowerPoint\Security 3. Ensure that the NoTBPromptUnsignedAddin DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office PowerPoint 2007\PowerPoint Options\Security\Trust Center 3. Double-Click Disable Trust Bar Notification for unsigned application add-ins. 4. Select Enabled, click OK.

Additional References
CCE-743-5

1.5.6. External Program Security

1.5.6.1. Prevent Active Buttons Running Programs: Level I

Description
The **Run Programs** option determines whether PowerPoint can utilize Run Programs option for action buttons.

Rationale
Setting this option to **disable - don't run any programs** reduces the attack surface of the application by preventing a malicious User can create an active button, potentially executing malicious code on a User's machine.

Settings: ..\Microsoft Office PowerPoint 2007\PowerPoint Options\Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**

Run Programs	Enabled disable - don't run any programs	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\PowerPoint\Security 3. Ensure that the RunPrograms DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office PowerPoint 2007\PowerPoint Options\Security 3. Double-Click Run Programs. 4. Select Enabled, select disable - don't run any programs, click OK.

Additional References
CCE-1649-3

1.5.7. Trusted Location Security

1.5.7.1. Require Local Trusted Locations: Level I

Description
The **Allow External Trusted Locations** option determines if locations on the network can be used as a Trusted Location.

Rationale
Files loaded into Trusted Locations may be controlled by malicious Users and are not subject to security measures. Setting this option to **Disabled** reduces the attack surface of PowerPoint by not allowing network locations to be regarded as Trusted Locations.

Settings: ..\Microsoft Office PowerPoint 2007\PowerPoint Options\Security\Trust Center\Trusted Locations				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Allow Trusted Locations not on the computer	Disabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select:

HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\PowerPoint\Security\Trusted Locations
3. Ensure that the AllowNetworkLocations DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office PowerPoint 2007\PowerPoint Options\Security\Trust Center\Trusted Locations 3. Double-Click Allow Trusted Locations not on the computer. 4. Select Disabled, click OK.

Additional References
CCE-747-6

1.5.7.2. Disable all Trusted Locations: Level II

Description
The **Disable all trusted locations** option determines if PowerPoint disables all Trusted Locations.

Rationale
Files loaded into Trusted Locations may be controlled by malicious Users and are not subject to security measures. Setting this option to **Enabled** reduces the attack surface by disabling all Trusted Locations.

Settings: ..\Microsoft Office PowerPoint 2007\PowerPoint Options\Security\Trust Center\Trusted Locations

Group Policy Object	Recommended State	Version	Level	Scorability
Disable all trusted locations	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\PowerPoint\Security\Trusted Locations 3. Ensure that the AllLocationsDisabled DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK.

2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office PowerPoint 2007\PowerPoint Options\Security\Trust Center\Trusted Locations 3. Double-Click Disable all trusted locations. 4. Select Enabled, click OK.

Additional References
CCE-782-3

1.5.7.3. Disable Slide Update: Level II

Description
The **Disable Slide Update** option determines if PowerPoint slides can be linked to a Slide Library, prompting the Users if changes occur.

Rationale
Setting this option to **Enabled** protects against a malicious attacker accessing the Slide Library with the intent of harming the integrity of the presentation.

Settings: ..\Microsoft Office PowerPoint 2007\Miscellaneous				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable Slide Update	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\PowerPoint\slide libraries 3. Ensure that the DisableSlideUpdate DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office PowerPoint 2007\Miscellaneous 3. Double-Click Disable Slide Update. 4. Select Enabled, click OK.

Additional References
CCE-1731-9

1.6. Access

1.6.1. Macro Security

1.6.1.1. Receive TrustBar Notifications when Macros Exist: Level I

Description
The **VBA Macro Warning Settings** option determines whether Office applications notify the User when VBA macros exist in a document.

Rationale
By default, Users can enable any macro manually through the Trust Bar. Enabling this option to **Trust Bar warning for all macros** prevents Users from enabling all macros.

Settings: ..\Microsoft Office Access 2007\Application Settings\Security\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
VBA Macro Warning Settings	Enabled Trust Bar warning for all macros	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Access\Security 3. Ensure that the VBAWarnings DWORD exists and is set to 2.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Access 2007\Application Settings\Security\Trust Center 3. Double-Click VBA Macro Warning Settings. 4. Select Enabled, select Trust Bar warning for all macros, and click OK.

Additional References
CCE-427-5

1.6.1.2. Receive TrustBar Notifications when Signed Macros Exist: Level II

Description
The **VBA Macro Warning Settings** option determines if Office applications notify the User when VBA macros exist in a document.

Rationale

By default, Users can enable any macro manually through the Trust Bar. A malicious User may use an unsigned macro in an attempt to gain code execution on a User's machine. Enabling this option to **Trust Bar warning for digitally signed macros only (unsigned macros will be disabled)** limits execution to signed macros, reducing the attack surface area of this application.

Settings: ..\Microsoft Office Access 2007\Application Settings\Security\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
VBA Macro Warning Settings	Enabled Trust Bar warning for digitally signed macros only (unsigned macros will be disabled)	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Access\Security 3. Ensure that the VBAWarnings DWORD exists and is set to 3.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Access 2007\Application Settings\Security\Trust Center 3. Double-Click VBA Macro Warning Settings. 4. Select Enabled, select Trust Bar warning for digitally signed macros only (unsigned macros will be disabled), click OK.

Additional References
CCE-427-5

1.6.2. File Conversion, Opening and Saving Security

1.6.2.1. Access Database Conversion Prompt: Level I

Description
The **Do not prompt to convert older databases** option determines whether Access prompts to convert older databases when they are opened.

Rationale
If this option is **Disabled**, a User is prompted upon opening an older database to convert to a newer version. Newer security features that exist in Access 2007 will not be available unless

the database is converted.

Settings: ..\Microsoft Office Access 2007\Miscellaneous				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Do not prompt to convert older databases	Disabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Access\Settings 3. Ensure that the NoConvertDialog DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Access 2007\Miscellaneous 3. Double-Click Do not prompt to convert older databases. 4. Select Disabled, click OK.

Additional References
CCE-1510-7

1.6.3. Add-In Security

1.6.3.1. Disable all Application Add-Ins: Level I

Description
The **Disable all application add-ins** setting determines if application add-ins are initialized.

Rationale
Application add-ins could potentially be used by a malicious User to gain code execution on a User's box. Setting this option to **Not Configured** will disable all application add-ins.

Settings: ..\Microsoft Office Access 2007\Application Settings\Security\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable all application add-ins	Not Configured	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Access\Security

3. Ensure that the DisableAllAddins DWORD does not exist.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Access 2007\Application Settings\Security\Trust Center 3. Double-Click Disable all application add-ins. 4. Select Not Configured, click OK.

Additional References
CCE-1238-5

1.6.3.2. Require Signed Application Add-Ins: Level II

Description
The **Require that application add-ins are signed by Trusted Publisher** option determines if application add-ins must be signed by a Trusted Publisher.

Rationale
A malicious User may use unsigned add-ins to gain code execution on a User's machine. Setting this option to **Enabled** will require that all executed add-ins must be signed by a Trusted Publisher.

Settings: ..\Microsoft Office Access 2007\Application Settings\Security\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Require that application add-ins are signed by Trusted Publisher	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Access\Security 3. Ensure that the RequireAddinSig DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Access 2007\Application Settings\Security\Trust Center 3. Double-Click Require that application add-ins are signed by Trusted Publisher. 4. Select Enabled, click OK.

Additional References
CCE-1476-1

1.6.3.3. TrustBar Notification for Unsigned Application Add-Ins: Level II

Description
The **Disable Trust Bar Notification for unsigned application add-ins** option determines whether Trust Bar Notifications are displayed when unsigned application add-ins are loaded, or whether they are silently disabled and prevented from executing.

Rationale
A malicious User may use unsigned add-ins to gain code execution on a User's machine. Setting this option to **Enabled** forces Access to automatically and silently disable unsigned application add-ins.

Settings: ..\Microsoft Office Access 2007\Application Settings\Security\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable Trust Bar Notification for unsigned application add-ins	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Access\Security 3. Ensure that the NoTBPromptUnsignedAddin DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Access 2007\Application Settings\Security\Trust Center 3. Double-Click Disable Trust Bar Notification for unsigned application add-ins. 4. Select Enabled, click OK.

Additional References
CCE-1423-3

1.6.4. Hyperlink Security

1.6.4.1. Underline Hyperlinks: Level II

Description
The **Underline hyperlinks** option determines whether hyperlinks in tables, queries, forms, and reports are underlined.

Rationale
Users may possibly click on dangerous URLs if hyperlinks are not underlined. Setting this option to **Enabled** underlines all hyperlinks in Access tables, queries, forms, and reports.

Settings: ..\Microsoft Office Access 2007\Application Settings\Web Options\General				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Underline hyperlinks	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Access\Internet 3. Ensure that the DoNotUnderlineHyperlinks DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Access 2007\Application Settings\Web Options\General 3. Double-Click Underline hyperlinks. 4. Select Enabled, click OK.

Additional References
CCE-1395-3

1.6.5. Trusted Location Security

1.6.5.1. External Trusted Locations: Level I

Description
The **Allow External Trusted Locations** option determines if locations on the network can be used as a Trusted Location.

Rationale
Files loaded into Trusted Locations may be controlled by malicious Users and are not subject to security measures. Setting this option to **Disabled** reduces the attack surface of Access by not allowing network locations to be regarded as Trusted Locations.

Settings: ..\Microsoft Office Access 2007\Application Settings\Security\Trust Center\Trusted Locations				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**

Allow Trusted Locations not on the computer	Disabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Access\Security\Trusted Locations 3. Ensure that the AllowNetworkLocations DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Access 2007\Application Settings\Security\Trust Center\Trusted Locations 3. Double-Click Allow Trusted Locations not on the computer. 4. Select Disabled, click OK.

Additional References
CCE-780-7

1.6.5.2. Disable all Trusted Locations: Level II

Description
The **Disable all trusted locations** option determines if Access disables all Trusted Locations.

Rationale
Files loaded into Trusted Locations may be controlled by malicious Users and are not subject to security measures. Setting this option to **Enabled** reduces the attack surface by disabling all Trusted Locations.

Settings: ..\Microsoft Office Access 2007\Application Settings\Security\Trust Center\Trusted Locations				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable all trusted locations	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Access\Security\Trusted

Locations
3. Ensure that the AllLocationsDisabled DWORD exists and is set to 1.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
   Microsoft Office Access 2007\Application Settings\Security\Trust Center\Trusted Locations
3. Double-Click Disable all trusted locations.
4. Select Enabled, click OK.

Additional References

CCE-1520-6

1.6.5.3. Untrusted Components Notification: Level II

Description

The **Modal Trust Decision Only** option determines if Access notifies a User about untrusted components within a database.

Rationale

By default, Access disables untrusted components but allows Users to selectively enable untrusted components if necessary. Setting this option to **Disabled** ensures that a User cannot reduce the security level of this setting through the application UI.

Settings: ..\Microsoft Office Access 2007\Tools | Security

Group Policy Object	Recommended State	Version	Level	Scorability
Modal Trust Decision Only	Disabled	2007	II	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Access\Security
3. Ensure that the ModalTrustDecisionOnly DWORD exists and is set to 0.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
   Microsoft Office Access 2007\Tools | Security
3. Double-Click Modal Trust Decision Only.
4. Select Disabled, click OK.

Additional References
CCE-1214-6

1.7. InfoPath

1.7.1. File Opening and Saving Security

1.7.1.1. Block Opening Solutions from an Internet Security Zone: Level I

Description
The **Disable opening of solutions from the Internet security zone** option determines whether a User can open a solution from an Internet security zone.

Rationale
Attackers may host malicious InfoPath solutions on the Internet to lure Users into inadvertently leaking sensitive data. Setting this option to **Enabled** will prevent a User from opening solutions from an Internet security zone.

Settings: ..\Microsoft Office InfoPath 2007\Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable opening of solutions from the Internet security zone	Enabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath\Security 3. Ensure that the AllowInternetSolutions DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office InfoPath 2007\Security 3. Double-Click Disable opening of solutions from the Internet security zone. 4. Select Enabled, click OK.

Additional References
CCE-1105-6

1.7.2. Code & Script Security

1.7.2.1. Opening a Fully Trusted Form: Level I

Description
The **Disable fully trusted solutions full access to computer** option determines whether an InfoPath User can open a fully trusted form.

Rationale
In InfoPath, fully trusted forms have the ability to access local system resources, including COM components or User files, as well as the suppression of security prompts. Enabling this option prevents malicious scripts from accessing these resources.

Settings: ..\Microsoft Office InfoPath 2007\Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable fully trusted solutions full access to computer	Enabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath\Security 3. Ensure that the RunFullTrustSolutions DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office InfoPath 2007\Security 3. Double-Click Disable fully trusted solutions full access to computer. 4. Select Enabled, click OK.

Additional References
CCE-1114

1.7.2.2. Custom Code in Forms: Level II

Description
The **Custom code** option determines whether a User can design an InfoPath form that uses custom code.

Rationale
Setting this option to **Enabled** restricts a malicious User from creating a malicious InfoPath form with custom C# or VisualBasic code that may harm another User's computer or data.

Settings: ..\Microsoft Office InfoPath 2007\Restricted Features				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Custom code	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath\ Designer\RestrictedFeatures 3. Ensure that the CodeAllowed DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office InfoPath 2007\Restricted Features 3. Double-Click Custom code. 4. Select Enabled, click OK.

Additional References
CCE-1564-4

1.7.3. Add-In Security

1.7.3.1. Disable all Application Add-Ins: Level I

Description
The **Disable all application add-ins** setting determines if application add-ins are initialized.

Rationale
Application add-ins could potentially be used by a malicious User to gain code execution on a User's box. Setting this option to **Not Configured** will disable all application add-ins.

Settings: ..\Microsoft Office InfoPath 2007\Security\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable all application add-ins	Not Configured	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath\Security 3. Ensure that the DisableAllAddins DWORD does not exist.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office InfoPath 2007\Security\Trust Center 3. Double-Click Disable all application add-ins. 4. Select Not Configured, click OK.

Additional References
CCE-1135-3

1.7.3.2. Require Signed Application Add-Ins: Level II

Description
The **Require that application add-ins are signed by Trusted Publisher** option determines if application add-ins must be signed by a Trusted Publisher.

Rationale
A malicious User may use unsigned add-ins to gain code execution on a User's machine. Setting this option to **Enabled** will require that all executed add-ins must be signed by a Trusted Publisher.

Settings: ..\Microsoft Office InfoPath 2007\Security\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Require that application add-ins are signed by Trusted Publisher	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath\Security 3. Ensure that the RequireAddinSig DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office InfoPath 2007\Security\Trust Center 3. Double-Click Require that application add-ins are signed by Trusted Publisher. 4. Select Enabled, click OK.

Additional References

CCE-1157-7

1.7.3.3. TrustBar Notification for Unsigned Application Add-Ins: Level II

Description
The **Disable Trust Bar Notification for unsigned application add-ins** option determines whether Trust Bar Notifications are displayed when unsigned application add-ins are loaded, or whether they are silently disabled and prevented from executing.

Rationale
A malicious User may use unsigned add-ins to gain code execution on a User's machine. Setting this option to **Enabled** forces InfoPath to automatically and silently disable unsigned application add-ins.

Settings: ..\Microsoft Office InfoPath 2007\Security\Trust Center				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable Trust Bar Notification for unsigned application add-ins	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath\Security 3. Ensure that the NoTBPromptUnsignedAddin DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office InfoPath 2007\Security\Trust Center 3. Double-Click Disable Trust Bar Notification for unsigned application add-ins. 4. Select Enabled, click OK.

Additional References
CCE-1434-0

1.7.4. Forms Security

1.7.4.1. Block Opening of Internet Form in InfoPath: Level I

Description
The **Control behavior when opening forms in the Internet security zone** option establishes the method InfoPath uses to open forms when there is a mismatch in the location between the form and the locally cached form that originate from the Internet.

Rationale
If InfoPath does not warn when there is a mismatch in the location information between the form and the locally cached form, a malicious User could potentially use form redirection as Web beaconing to determine information about a User. Enabling this option to block will block requests for a form if a mismatch exists.

Settings: ..\Microsoft Office InfoPath 2007\Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Control behavior when opening forms in the Internet security zone	Enabled Block	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath\Open Behaviors 3. Ensure that the Internet DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office InfoPath 2007\Security 3. Double-Click Control behavior when opening forms in the Internet security zone. 4. Select Enabled, select Block, and click OK.

Additional References
CCE-1479-5

1.7.4.2. Block Opening of Intranet Form in InfoPath: Level I

Description
The **Control behavior when opening forms in the Intranet security zone** option determines whether InfoPath will open a form that originates from the Intranet when a mismatch occurs in the location information between the form and the locally cached form.

Rationale
If InfoPath does not warn a mismatch occurs in the location information between the form and the locally cached form, a malicious User can use form redirection as Web beaconing to determine information about a User. Enabling this option to block will block requests for a form if a mismatch exists.

Settings: ..\Microsoft Office InfoPath 2007\Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Control behavior when opening forms in the Intranet security zone	Enabled Block	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath\Open Behaviors 3. Ensure that the Intranet DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office InfoPath 2007\Security 3. Double-Click Control behavior when opening forms in the Intranet security zone. 4. Select Enabled, select Block, and click OK.

Additional References
CCE-1360-7

1.7.4.3. Block Opening of a Trusted Site Form in InfoPath: Level I

Description
The **Control behavior when opening forms in the Trusted Site security zone** option determines how InfoPath will open forms when there is a mismatch in the location information between the form and a locally cached form that originate from Trusted Site security zones.

Rationale
If InfoPath does not warn when there is a mismatch in the location information between the form and the locally cached form, a malicious User may use form redirection as Web beaconing to determine information about a User. Enabling this option to **Block** will not allow requests for a form if such a mismatch exists.

Settings: ..\Microsoft Office InfoPath 2007\Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Control behavior when opening forms in the Trusted Site security zone	Enabled Block	2007	I	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath\Open Behaviors
3. Ensure that the Trusted Site DWORD exists and is set to 0.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
   Microsoft Office InfoPath 2007\Security
3. Double-Click Control behavior when opening forms in the Trusted Site security zone.
4. Select Enabled, select Block, and click OK.

Additional References

CCE-893-8

1.7.4.4. Prompt Before Opening Forms that Contain Code or Script: Level I

Description

The **Control behavior when opening InfoPath e-mail forms containing code or script** option determines whether InfoPath opens forms that contain code or scripts.

Rationale

InfoPath forms may potentially contain malicious code or scripts which can execute on a User's machine. By default, Users are prompted before executing code or scripts. However, if this option not explicitly set to **Enabled - Prompt before running**, Users can set this option to a less secure state.

Settings: ..\Microsoft Office InfoPath 2007\InfoPath e-mail forms

Group Policy Object	Recommended State	Version	Level	Scorability
Control behavior when opening InfoPath e-mail forms containing code or script	Enabled Prompt before running	2007	I	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath\Security
3. Ensure that the EMailFormsRunCodeAndScript DWORD exists and is set to 1.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.

2. Locate and select:
   User Configuration\Administrative Templates\
      Microsoft Office InfoPath 2007\InfoPath e-mail forms
3. Double-Click Control behavior when opening InfoPath e-mail forms containing code or script.
4. Select Enabled, select Prompt before running, click OK.

Additional References
CCE-1315-1

1.7.4.5. Prevent Before Opening Forms that Contain Code or Script: Level II

Description
The **Control behavior when opening InfoPath e-mail forms containing code or script** option determines whether InfoPath opens forms that contain code or scripts.

Rationale
InfoPath forms may potentially contain malicious code or scripts which can execute on a User's machine. Setting this option to **Enabled – Never Run**, will not run any code or scripts contained in InfoPath forms.

Settings: ..\Microsoft Office InfoPath 2007\InfoPath e-mail forms				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Control behavior when opening InfoPath e-mail forms containing code or script	Enabled Never run	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath\Security 3. Ensure that the EMailFormsRunCodeAndScript DWORD exists and is set to 2.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office InfoPath 2007\InfoPath e-mail forms 3. Double-Click Control behavior when opening InfoPath e-mail forms containing code or script. 4. Select Enabled, select Never run, click OK.

Additional References

CCE-1315-1

1.7.4.6. Dynamic Caching of Form Templates: Level II

Description
The **Disable dynamic caching of the form template in InfoPath e-mail forms** option determines if InfoPath caches local copies of form templates received with e-mail forms.

Rationale
Caching of form templates can circumvent a User filling out a properly published form, potentially leaking sensitive data to a malicious User instead of the intended Recipient. Setting this option to **Enabled** caches the published version of the form template instead of the template included with the e-mail form.

Settings: ..\Microsoft Office InfoPath 2007\InfoPath e-mail forms				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable dynamic caching of the form template in InfoPath e-mail forms	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath\Deployment 3. Ensure that the CacheMailXSN DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office InfoPath 2007\InfoPath e-mail forms 3. Double-Click Disable dynamic caching of the form template in InfoPath e-mail forms. 4. Select Enabled, click OK.

Additional References
CCE-1236-9

1.7.4.7. Block Restricted Email Forms: Level II

Description
The **Disable e-mail forms running in restricted security level** option determines whether an e-mail form that runs at restricted security levels can be opened.

Rationale

While InfoPath forms that run with a restricted security level can only access data that is stored in the form, a malicious User could potentially craft an e-mail form that leaks sensitive data if filled out by a User. Setting this option to **Enabled** will disable running forms in restricted security levels.

Group Policy Object	Recommended State	Version	Level	Scorability
Disable e-mail forms running in restricted security level	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath\Security 3. Ensure that the EnableRestrictedEMailForms DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office InfoPath 2007\InfoPath e-mail forms 3. Double-Click Disable e-mail forms running in restricted security level. 4. Select Enabled, click OK.

Additional References
CCE-1518-0

1.7.4.8. Block Internet Email Forms: Level I

Description
The **Disable e-mail forms from the Internet security zone** option determines whether InfoPath will open an e-mail form that originates from the Internet.

Rationale
A malicious User could potentially craft an e-mail form that leaks sensitive data if filled out by a User. Setting this option to **Enabled** prevents opening an e-mail form which originates from the Internet.

Settings: ..\Microsoft Office InfoPath 2007\InfoPath e-mail forms				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable e-mail forms from the Internet security zone	Enabled	2007	I	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath\Security
3. Ensure that the EnableInternetEMailForms DWORD exists and is set to 1.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
      Microsoft Office InfoPath 2007\InfoPath e-mail forms
3. Double-Click Disable e-mail forms from the Internet security zone.
4. Select Enabled, click OK.

Additional References

CCE-1170-0

1.7.4.9. Block Intranet Email Forms: Level II

Description

The **Disable e-mail forms from the Intranet security zone** option determines whether InfoPath will open an e-mail form that originates from the Intranet.

Rationale

A malicious User could potentially craft an e-mail form that leaks sensitive data if filled out by a User. Setting this option to **Enabled** prevents InfoPath opening e-mail forms from the Intranet.

Settings: ..\Microsoft Office InfoPath 2007\InfoPath e-mail forms

Group Policy Object	Recommended State	Version	Level	Scorability
Disable e-mail forms from the Intranet security zone	Enabled	2007	II	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath\Security
3. Ensure that the EnableIntranetEMailForms DWORD exists and is set to 1.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
      Microsoft Office InfoPath 2007\InfoPath e-mail forms

3. Double-Click Disable e-mail forms from the Intranet security zone. 4. Select Enabled, click OK.

Additional References
CCE-1316-9

1.7.4.10. Block fully trusted email forms: Level I

Description
The **Disable e-mail forms from the Full Trust security zone** option determines whether a User can open a fully trusted form.

Rationale
Setting this option to **Enabled** prevents potentially malicious scripts from accessing local system resources, such as COM components, files on a User's computer, or potentially suppressing security prompts.

Settings: ..\Microsoft Office InfoPath 2007\InfoPath e-mail forms				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable e-mail forms from the Full Trust security zone	Enabled	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath\Security 3. Ensure that the EnableFullTrustEmailForms DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office InfoPath 2007\InfoPath e-mail forms 3. Double-Click Disable e-mail forms from the Full Trust security zone. 4. Select Enabled, click OK.

Additional References
CCE-1567-7

1.7.4.11. Do not automatically render InfoPath forms in outlook: Level II

Description
The **Disable InfoPath e-mail forms in Outlook** option determines whether Outlook will automatically render InfoPath e-mail forms or attachments.

Rationale
A malicious User can send InfoPath e-mail forms in an attempt to gain access to confidential information. Depending on the level of trust of the forms, it might also be possible to gain access to other data automatically. Setting this option to **Enabled** prevents Outlook from rendering InfoPath forms.

Settings: ..\Microsoft Office InfoPath 2007\InfoPath e-mail forms				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Disable InfoPath e-mail forms in Outlook	Enabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Options\Mail 3. Ensure that the DisableInfopathForms DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office InfoPath 2007\InfoPath e-mail forms 3. Double-Click Disable InfoPath e-mail forms in Outlook. 4. Select Enabled, click OK.

Additional References
CCE-1265-8

1.7.5. External Content Security

1.7.5.1. Prevent InfoPath Web Beacons to Internet Zone: Level I

Description
The **Beaconing UI for forms opened in InfoPath** option determines whether Users are prompted with a security warning when openning InfoPath forms that contain a Web beacon.

Rationale
Web beaconing can be used to send any data collected by the InfoPath forms to an external server, potentially leaking sensitive information. Setting the option to **Show UI if form template is in Internet Zone** will prompt about beaconing threats if data transfer would cause data to be sent to an Internet Zone.

Settings: ..\Microsoft Office InfoPath 2007\Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Beaconing UI for forms opened in InfoPath	Enabled Show UI if form template is from Internet Zone	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath\Security 3. Ensure that the InfoPathBeaconingUI DWORD exists and is set to 2.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office InfoPath 2007\Security 3. Double-Click Beaconing UI for forms opened in InfoPath. 4. Select Enabled, select Show UI if form template is from Internet Zone, and click OK.

Additional References
CCE-1290-6

1.7.5.2. Prevent InfoPath Web Beacons to any Zone: Level II

Description
The **Beaconing UI for forms opened in InfoPath** option determines whether Users see a security warning when they open InfoPath forms that contain a Web beaconing threat.

Rationale
Web beaconing can be used to send any data collected by the InfoPath forms to an external server, potentially leaking sensitive information. Setting the option to **Always show beaconing UI** will prompt about Beaconing threats when one is detected.

Settings: ..\Microsoft Office InfoPath 2007\Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Beaconing UI for forms opened in InfoPath	Enabled Always show beaconing UI	2007	II	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath\Security
3. Ensure that the InfoPathBeaconingUI DWORD exists and is set to 1.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
   Microsoft Office InfoPath 2007\Security
3. Double-Click Beaconing UI for forms opened in InfoPath.
4. Select Enabled, select Always show beaconing UI, click OK.

Additional References

CCE-1290-6

1.7.5.3. Prevent InfoPath ActiveX Web Beacons to Internet Zone: Level I

Description

The **Beaconing UI for forms opened in InfoPath Editor ActiveX** option determines whether Users are prompted with a security warning when opening an InfoPath form control that contains a Web beacon.

Rationale

Web beaconing can be used to send any data collected by the InfoPath forms to an external server, potentially leaking sensitive information. Setting the option to **Show UI if form template is in Internet Zone** will prompt about Beaconing threats if the data transfer would cause data to be sent to an Internet Zone.

Settings: ..\Microsoft Office InfoPath 2007\Security

Group Policy Object	Recommended State	Version	Level	Scorability
Beaconing UI for forms opened in InfoPath Editor ActiveX	Enabled Show UI if form template is from Internet Zone	2007	I	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath\Security
3. Ensure that the EditorActiveXBeaconingUI DWORD exists and is set to 2.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.

2. Locate and select:
   User Configuration\Administrative Templates\
      Microsoft Office InfoPath 2007\Security
3. Double-Click Beaconing UI for forms opened in InfoPath Editor ActiveX.
4. Select Enabled, select Show UI if form template is from Internet Zone, and click OK.

Additional References

CCE-1381-3

1.7.5.4. Prevent InfoPath ActiveX Web Beacons to any zone: Level II

Description

The **Beaconing UI for forms opened in InfoPath Editor ActiveX** option determines whether Users are prompted with a security warning when opening an InfoPath form control that contains a Web beacon.

Rationale

Web beaconing can be used to send any data collected by the InfoPath forms to an external server, potentially leaking sensitive information. Setting the option to **Always show beaconing UI** will prompt about Beaconing threats when one is detected.

Settings: ..\Microsoft Office InfoPath 2007\Security

Group Policy Object	Recommended State	Version	Level	Scorability
Beaconing UI for forms opened in InfoPath Editor ActiveX	Enabled Always show beaconing UI	2007	II	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath\Security
3. Ensure that the EditorActiveXBeaconingUI DWORD exists and is set to 1.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
      Microsoft Office InfoPath 2007\Security
3. Double-Click Beaconing UI for forms opened in InfoPath Editor ActiveX.
4. Select Enabled, select Always show beaconing UI, click OK.

Additional References

CCE-1381-3

1.7.5.5. Prevent InfoPath Email Form Web Beacons to Internet Zone: Level I

Description
The **Email Forms Beaconing UI** option determines whether Users see a security warning when they open an InfoPath e-mail form that contains a Web beaconing threat.

Rationale
Web beaconing can be used to send any data collected by the InfoPath forms to an external server, potentially leaking sensitive information. Setting the option to **Show UI if XSN is in Internet Zone** will prompt about beaconing threats if the data transfer would cause data to be sent to an Internet Zone.

Settings: ..\Microsoft Office InfoPath 2007\Miscellaneous				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Email Forms Beaconing UI	Enabled Show UI if XSN is in Internet Zone	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath\Security 3. Ensure that the EmailFormsBeaconingUI DWORD exists and is set to 2.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office InfoPath 2007\Miscellaneous 3. Double-Click Email Forms Beaconing UI. 4. Select Enabled, select Show UI if XSN is in Internet Zone, and click OK.

Additional References
CCE-1212-0

1.7.5.6. Prevent InfoPath Email Form Web Beacons to any Zone: Level II

Description
The **Email Forms Beaconing UI** option determines whether Users see a security warning when they open an InfoPath e-mail form that contains a Web beaconing threat.

Rationale
Web beaconing can be used to send any data collected by the InfoPath forms to an external server, potentially leaking sensitive information. Setting the option to **Always show UI** will

only be prompt about Beaconing threats anytime one is detected.

Settings: ..\Microsoft Office InfoPath 2007\Miscellaneous				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Email Forms Beaconing UI	Enabled Always show UI	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath\Security 3. Ensure that the EmailFormsBeaconingUI DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office InfoPath 2007\Miscellaneous 3. Double-Click Email Forms Beaconing UI. 4. Select Enabled, select Always show UI, and click OK.

Additional References
CCE-1212-0

1.7.6. Miscellaneous

1.7.6.1. Do not cache queries when InfoPath is offline: Level I

Description
The **Offline Mode status** option determines the behavior of InfoPath when Offline.

Rationale
By default, in offline mode, Users can cache queries for execution when InfoPath returns Online. If these queries contain sensitive information, the data could be at risk. Setting this option to **Enabled InfoPath not in Offline Mode** allows offline mode but does not let a User cache queries.

Settings: ..\Microsoft Office InfoPath 2007\Tools | Options\Advanced\Offline				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Offline Mode status	Enabled Enabled InfoPath not in Offline Mode	2007	I	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath\Editor\Offline 3. Ensure that the CachedModeStatus DWORD exists and is set to 2.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office InfoPath 2007\Tools | Options\Advanced\Offline 3. Double-Click Offline Mode status. 4. Select Enabled, select Enabled InfoPath not in Offline Mode, and click OK.

Additional References
CCE-569-4

1.7.6.2. Disable InfoPath offline mode: Level II

Description
The **Offline Mode status** option determines the behavior of InfoPath when Offline.

Rationale
By default, in offline mode, Users can cache queries for execution when InfoPath returns Online. If these queries contain sensitive information, the data could be at risk. Disabling Offline mode eliminates this risk.

Settings: ..\Microsoft Office InfoPath 2007\Tools | Options\Advanced\Offline				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Offline Mode status	Enabled Disabled	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath\Editor\Offline 3. Ensure that the CachedModeStatus DWORD exists and is set to 0.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK.

2. Locate and select:
   User Configuration\Administrative Templates\
      Microsoft Office InfoPath 2007\Tools | Options\Advanced\Offline
3. Double-Click Offline Mode status.
4. Select Enabled, select Disabled, and click OK.

Additional References

CCE-569-4

1.7.6.3. Allow only Intranet redirections during SharePoint upgrade: Level I

Description

The **Control behavior for Windows SharePoint Services gradual upgrade** option determines whether forms and form templates follow URL redirections provided by a SharePoint service during an upgrade.

Rationale

By automatically redirecting forms and form templates, a User may inadvertently be redirected to an insecure site and may leak sensitive information. Setting this option to **Allow redirections to Intranet only** provides reasonable assurances that data will stay within an enterprise, while being more useable.

Settings: ..\Microsoft Office InfoPath 2007\Security

Group Policy Object	Recommended State	Version	Level	Scorability
Control behavior for Windows SharePoint Services gradual upgrade	Enabled Allow redirections to Intranet only	2007	I	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath\Security
3. Ensure that the GradualUpgradeRedirection DWORD exists and is set to 1.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
      Microsoft Office InfoPath 2007\Security
3. Double-Click Control behavior for Windows SharePoint Services gradual upgrade.
4. Select Enabled, select Allow redirections to Intranet only, click OK.

Additional References

CCE-704-7

1.7.6.4. Prevent all redirections during SharePoint upgrade: Level II

Description
This option determines whether forms and form templates follow URL redirections provided by a SharePoint service during an upgrade.

Rationale
Setting this option to **Block all redirections** prevents automatically redirecting forms and form templates, inadvertently redirecting a User to an insecure site potentially leaking sensitive information.

Settings: ..\Microsoft Office InfoPath 2007\Security				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Control behavior for Windows SharePoint Services gradual upgrade	Enabled Block all redirections	2007	II	S

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath\Security 3. Ensure that the GradualUpgradeRedirection DWORD exists and is set to 2.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office InfoPath 2007\Security 3. Double-Click Control behavior for Windows SharePoint Services gradual upgrade. 4. Select Enabled, select Block all redirections, click OK.

Additional References
CCE-704-7

1.7.6.5. Allow Information Rights Management: Level I

Description
This option determines whether a User can create an IRM protected form.

Rationale
Disabling this setting allows Users to create IRM protected forms. IRM can be used to increase security by restricting the people authorized to view a specific document.

Settings: ..\Microsoft Office InfoPath 2007\Restricted Features				
Group Policy Object	**Recommended State**	**Version**	**Level**	**Scorability**
Information Rights Management	Disabled	2007	I	S

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath\
   Designer\RestrictedFeatures
3. Ensure that the IRMAllowed DWORD exists and is set to 1.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
   Microsoft Office InfoPath 2007\Restricted Features
3. Double-Click Information Rights Management.
4. Select Disabled, click OK.

Additional References

CCE-1538-8

2. Informational Settings

2.1. Informational Settings for Office 2003

2.1.1.1. User Configuration for Source S/MIME Certificate

Description
Outlook directs to a page on the Microsoft Office Online Web site where Users can obtain S/MIME certificates for encryption and signing if a User clicks **Get a Digital ID** in the **E-mail Security** section of the Trust Center. Enabling this configuration might allow Users to violate policies that manage the use of external resources like Office Online.

Rationale
This informational option is for enterprise administrators that have a URL to supply for S/MIME certificates.

Settings: ..\Microsoft Office Outlook 2003\Tools | Options...\Security\Cryptography			
Group Policy Object	**Recommended State**	**Version**	**Scorability**
URL for S/MIME certificates	Not Configured	2003	Y

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\11.0\Outlook\Security 3. Ensure that the EnrollPageURL DWORD does not exist.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2003\Tools | Options...\Security\Cryptography 3. Double-Click URL for S/MIME certificates. 4. Select Not Configured, click OK.

2.1.1.2. User Configuration of Required Certificate Authority

Description
Outlook has the ability to trust certificate authorities in the Trusted Root Certificate Authorities store on User's computers.

Rationale

This informational option is for administrators who have a certificate authority supply for encryption and digital signatures. Enabling this option will allow administrators to delegate a certificate authority for Outlook to use for encryption and digital signatures

Settings: ..\Microsoft Office Outlook 2003\Tools | Options...\Security\Cryptography			
Group Policy Object	**Recommended State**	**Version**	**Scorability**
Required Certificate Authority	Not Configured	2003	Y

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\11.0\Outlook\Security 3. Ensure that the RequiredCA SZ does not exist.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2003\Tools | Options...\Security\Cryptography 3. Double-Click Required Certificate Authority. 4. Select Not Configured, click OK.

2.1.1.3. User Configuration for Encrypting All E-mails

Description
Leaving this option not configured allows administrators to require that all e-mail messages be encrypted when sent from Outlook.

Rationale
Clear text e-mails are vulnerable when intercepted. This informational option allows organizations with very strong security requirements to force Users encrypt all outbound e-mail messages.

Settings: ..\Microsoft Office Outlook 2003\Tools | Options...\Security\Cryptography			
Group Policy Object	**Recommended State**	**Version**	**Scorability**
Encrypt all e-mail messages	Not Configured	2003	Y

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\11.0\Outlook\Security 3. Ensure that the AlwaysEncrypt DWORD does not exist.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2003\Tools | Options...\Security\Cryptography 3. Double-Click Encrypt all e-mail messages. 4. Select Not Configured, click OK.

2.1.1.4. Allow User Configuration for Fortezza Certificate Policies

Description
This setting will create a list of policies allowed in the extension of Fortezza certificates, a hardware level encryption method created by the National Security Agency.

Rationale
Setting this informational option will allow administrators to configure Fortezza certificates.

Settings: ..\Microsoft Office Outlook 2003\Tools | Options...\Security\Cryptography			
Group Policy Object	**Recommended State**	**Version**	**Scorability**
Fortezza certificate policies	Not Configured	2003	Y

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\11.0\Outlook\Security 3. Ensure that the Fortezza_Policies DWORD does not exist.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2003\Tools | Options...\Security\Cryptography 3. Double-Click Fortezza certificate policies. 4. Select Not Configured, click OK.

2.1.1.5. User Configuration of FIPS Compliance

Description
This option determines whether Outlook uses FIPS compliant algorithms for signing and encrypting messages.

Rationale
This setting is information for system administrators that must configure Outlook to comply with standards for doing business with the U.S. government. Enabling this option causes Outlook to run in a mode that uses SHA1 for signing and 3DES for encryption.

Settings: ..\Microsoft Office Outlook 2003\Tools | Options...\Security\Cryptography			
Group Policy Object	**Recommended State**	**Version**	**Scorability**
Run in FIPS compliant mode	Not Configured	2003	Y

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\11.0\Outlook\Security 3. Ensure that the FIPSMode DWORD does not exist.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2003\Tools | Options...\Security\Cryptography 3. Double-Click Run in FIPS compliant mode. 4. Select Not Configured, click OK.

2.1.1.6. User Configuration to Disable Excel Commands

Description
This option can be used to disable specific Excel commands.

Rationale
This option is listed for informational purposes so that enterprise administrators can determine what commands, if any, should be disabled within the enterprise environment.

Settings: ..\Microsoft Office Excel 2003\Disable items in User interface\Predefined			
Group Policy Object	**Recommended State**	**Version**	**Scorability**
Disable commands	Not Configured	2003	Y

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\11.0\Excel 3. Ensure that the DisabledCmdBarItemsCheckBoxes key does not exist.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Excel 2003\Disable items in User interface\Predefined 3. Double-Click Disable commands. 4. Select Not Configured, click OK.

2.1.1.7. Disable Specific Word Commands

Description
This option can be used to disable specific Word commands.

Rationale
This informational option allows administrators can determine what commands should or should not be disabled within the enterprise environment.

Settings: ..\Microsoft Office Word 2003\Disable items in User interface\Predefined			
Group Policy Object	**Recommended State**	**Version**	**Scorability**
Disable commands	Not Configured	2003	Y

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\11.0\Word 3. Ensure that the DisabledCmdBarItemsCheckBoxes key does not exist.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Word 2003\Disable items in User interface\Predefined 3. Double-Click Disable commands. 4. Select Not Configured, click OK.

2.1.1.8. Disabling Specific PowerPoint commands

Description
This option can be used to disable specific PowerPoint commands.

Rationale
Setting this informational option will allow enterprise administrators to determine which

commands should or should not be disabled within the enterprise environment.

Settings: ..\Microsoft Office PowerPoint 2003\Disable items in User interface\Predefined			
Group Policy Object	**Recommended State**	**Version**	**Scorability**
Disable commands	Not Configured	2003	Y

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\11.0\PowerPoint 3. Ensure that the DisabledCmdBarItemsCheckBoxes key does not exist.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office PowerPoint 2003\Disable items in User interface\Predefined 3. Double-Click Disable commands. 4. Select Not Configured, click OK.

2.1.1.9. Disable Access Commands

Description
This option can be used to disable specific Access commands.

Rationale
This option is listed for informational purposes so that enterprise administrators can determine what commands, if any, should be disabled within the enterprise environment.

Settings: ..\Microsoft Office Access 2003\Disable items in User interface\Predefined			
Group Policy Object	**Recommended State**	**Version**	**Scorability**
Disable command bar buttons and menu items	Not Configured	2003	Y

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\11.0\Access 3. Ensure that the DisabledCmdBarItemsCheckBoxes key does not exist.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
   Microsoft Office Access 2003\Disable items in User interface\Predefined
3. Double-Click Disable command bar buttons and menu items.
4. Select Not Configured, click OK.

2.1.1.10. Adding File Type to InfoPath Forms as Attachments

Description
This setting controls which file types (determined by file extension) can be added to InfoPath forms as attachments.

Rationale
Enterprises with a policy requiring only certain types of attachments to be sent between Users can use this option to ensure conformance to this policy. This setting is informational.

Settings: ..\Microsoft Office InfoPath 2003\Security			
Group Policy Object	**Recommended State**	**Version**	**Scorability**
Allow file types as attachments to forms	Not Configured	2003	Y

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\11.0\InfoPath\Security 3. Ensure that the UnsafeFileTypesRemove SZ does not exist.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office InfoPath 2003\Security 3. Double-Click Allow file types as attachments to forms. 4. Select Not Configured, click OK.

2.1.1.11. Disable Specific InfoPath Commands

Description
This option can be used to disable specific InfoPath commands.

Rationale
This option is listed for informational purposes so that enterprise administrators can

determine what commands, if any, should be disabled within the enterprise environment.

Settings: ..\Microsoft Office InfoPath 2003\Disable items in User interface\Custom			
Group Policy Object	**Recommended State**	**Version**	**Scorability**
Disable commands	Not Configured	2003	Y

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\11.0\InfoPath 3. Ensure that the DisabledCmdBarItemsCheckBoxes key does not exist.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office InfoPath 2003\Disable items in User interface\Custom 3. Double-Click Disable commands. 4. Select Not Configured, click OK.

2.2. Informational Settings for Office 2007

2.2.1.1. Post Blog Entries

Description
The **Control Blogging** option determines whether Office applications can post blog entries directly to the Internet.

Rationale
This option is listed as informational. Enterprise environments that have policies regulating the publishing of data to external web sites may configure this option to disable blogging features in Office applications.

Settings: ..\Microsoft Office 2007 system\Miscellaneous			
Group Policy Object	**Recommended State**	**Version**	**Scorability**
Control Blogging	Enabled All blogging disabled	2007	Y

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Common\Blog

3. Ensure that the DisableBlog DWORD exists and is set to 2.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office 2007 system\Miscellaneous 3. Double-Click Control Blogging. 4. Select Enabled, select All blogging disabled, click OK.

Additional References
CCE-1241-9

2.2.1.2. URL for Certificates

Description
By default, when Users click **Get a Digital ID** in the **E-mail Security** section of the Trust Center, Outlook opens a page on the Microsoft Office Online Web site where they can obtain S/MIME certificates for encryption and signing. If an organization's policies govern the use of external resources like Office Online, this configuration might allow Users to violate those policies.

Rationale
This option is included as information for enterprise administrators that have a URL to supply for S/MIME certificates.

Settings: ..\Microsoft Office Outlook 2007\Security\Cryptography			
Group Policy Object	**Recommended State**	**Version**	**Scorability**
URL for S/MIME certificates	Not Configured	2007	Y

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the EnrollPageURL DWORD does not exist.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Cryptography 3. Double-Click URL for S/MIME certificates. 4. Select Not Configured, click OK.

Additional References
CCE-677-5

2.2.1.3. Fortezza Certificate Policies

Description
This setting specifies a list of policies allowed in the policies extension of a certificate that indicate the certificate is a Fortezza certificate.

Rationale
This option is included as information for administrators that need to configure Fortezza certificates.

Settings: ..\Microsoft Office Outlook 2007\Security\Cryptography			
Group Policy Object	**Recommended State**	**Version**	**Scorability**
Fortezza certificate policies	Not Configured	2007	Y

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the Fortezza_Policies DWORD does not exist.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Cryptography 3. Double-Click Fortezza certificate policies. 4. Select Not Configured, click OK.

Additional References
CCE-1402-7

2.2.1.4. Required Certificate Authority

Description
This option enables administrators to designate a required certificate authority for Outlook to use for encryption and digital signatures.

Rationale
This option is included as information for enterprise administrators that have a certificate authority to supply for encryption and digital signatures.

Settings: ..\Microsoft Office Outlook 2007\Security\Cryptography			
Group Policy Object	**Recommended State**	**Version**	**Scorability**
Required Certificate Authority	Not Configured	2007	Y

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the RequiredCA SZ does not exist.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Cryptography 3. Double-Click Required Certificate Authority. 4. Select Not Configured, click OK.

Additional References
CCE-1498-5

2.2.1.5. Run in FIPS Compliant Mode

Description
This option determines whether Outlook uses FIPS compliant algorithms for signing and encrypting messages.

Rationale
This setting is information for system administrators that must configure Outlook to comply with standards for doing business with the U.S. government. Enabling this option causes Outlook to run in a mode that uses SHA1 for signing and 3DES for encryption.

Settings: ..\Microsoft Office Outlook 2007\Security\Cryptography			
Group Policy Object	**Recommended State**	**Version**	**Scorability**
Run in FIPS compliant mode	Not Configured	2007	Y

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the FIPSMode DWORD does not exist.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Cryptography 3. Double-Click Run in FIPS compliant mode. 4. Select Not Configured, click OK.

Additional References
CCE-1018-1

2.2.1.6. Encrypt All E-Mail Messages

Description
This option allows administrators to require that all e-mail messages be encrypted when sent from Outlook.

Rationale
Most e-mail messages are sent in clear text, which leaves them vulnerable to interception. When stronger security is required, Users can encrypt messages with digital certificates so that they can only be read by the intended Recipients. This option is listed as informational; organizations with very strong security requirements might wish to require that Users encrypt all e-mail messages that they send.

Settings: ..\Microsoft Office Outlook 2007\Security\Cryptography			
Group Policy Object	**Recommended State**	**Version**	**Scorability**
Encrypt all e-mail messages	Not Configured	2007	Y

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Outlook\Security 3. Ensure that the AlwaysEncrypt DWORD does not exist.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Outlook 2007\Security\Cryptography 3. Double-Click Encrypt all e-mail messages. 4. Select Not Configured, click OK.

Additional References

CCE-1181-7

2.2.1.7. Disable Specific Word Commands

Description
This option can be used to disable specific Word commands.

Rationale
This option is listed for informational purposes so that enterprise administrators can determine what commands, if any, should be disabled within the enterprise environment.

Settings: ..\Microsoft Office Word 2007\Disable items in User interface\Predefined			
Group Policy Object	**Recommended State**	**Version**	**Scorability**
Disable commands	Not Configured	2007	Y

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Word 3. Ensure that the DisabledCmdBarItemsCheckBoxes key does not exist.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Word 2007\Disable items in User interface\Predefined 3. Double-Click Disable commands. 4. Select Not Configured, click OK.

Additional References
1. http://www.microsoft.com/technet/security/guidance/clientsecurity/2007office/tandc/default.mspx

2.2.1.8. Disable Specific PowerPoint Commands

Description
This option can be used to disable specific PowerPoint commands.

Rationale
This option is listed for informational purposes so that enterprise administrators can determine what commands, if any, should be disabled within the enterprise environment.

Settings: ..\Microsoft Office PowerPoint 2007\Disable items in User interface\Predefined

Group Policy Object	Recommended State	Version	Scorability
Disable commands	Not Configured	2007	Y

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\PowerPoint
3. Ensure that the DisabledCmdBarItemsCheckBoxes key does not exist.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
   Microsoft Office PowerPoint 2007\Disable items in User interface\Predefined
3. Double-Click Disable commands.
4. Select Not Configured, click OK.

Additional References

1. http://www.microsoft.com/technet/security/guidance/clientsecurity/2007office/tandc/default.mspx

2.2.1.9. Disable Specific Access Commands

Description

This option can be used to disable specific Access commands.

Rationale

This option is listed for informational purposes so that enterprise administrators can determine what commands, if any, should be disabled within the enterprise environment.

Settings: ..\Microsoft Office Access 2007\Disable items in User interface\Predefined

Group Policy Object	Recommended State	Version	Scorability
Disable commands	Not Configured	2007	Y

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Access
3. Ensure that the DisabledCmdBarItemsCheckBoxes key does not exist.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.

2. Locate and select:
   User Configuration\Administrative Templates\
      Microsoft Office Access 2007\Disable items in User interface\Predefined
3. Double-Click Disable commands.
4. Select Not Configured, click OK.

Additional References

1. http://www.microsoft.com/technet/security/guidance/clientsecurity/2007office/tandc/default.mspx

2.2.1.10. Disable Specific Excel Commands

Description

This option can be used to disable specific Excel commands.

Rationale

This option is listed for informational purposes so that enterprise administrators can determine what commands, if any, should be disabled within the enterprise environment.

Settings: ..\Microsoft Office Excel 2007\Disable items in User interface\Predefined

Group Policy Object	Recommended State	Version	Scorability
Disable commands	Not Configured	2007	Y

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Excel
3. Ensure that the DisabledCmdBarItemsCheckBoxes key does not exist.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
      Microsoft Office Excel 2007\Disable items in User interface\Predefined
3. Double-Click Disable commands.
4. Select Not Configured, click OK.

Additional References

1. http://www.microsoft.com/technet/security/guidance/clientsecurity/2007office/tandc/default.mspx

2.2.1.11. Disable Specific InfoPath Commands

Description
This option can be used to disable specific InfoPath commands.

Rationale
This option is listed for informational purposes so that enterprise administrators can determine what commands, if any, should be disabled within the enterprise environment.

Settings: ..\Microsoft Office InfoPath 2007\Disable items in User interface\Predefined			
Group Policy Object	**Recommended State**	**Version**	**Scorability**
Disable commands	Not Configured	2007	N

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath 3. Ensure that the DisabledCmdBarItemsCheckBoxes key does not exist.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office InfoPath 2007\Disable items in User interface\Predefined 3. Double-Click Disable commands. 4. Select Not Configured, click OK.

Additional References
1. http://www.microsoft.com/technet/security/guidance/clientsecurity/2007office/tandc/default.mspx

2.2.1.12. Determine Allowed File Types Attached to InfoPath Forms

Description
This setting controls which file types (determined by file extension) can be added to InfoPath forms as attachments.

Rationale
This setting is informational. Enterprises with a policy requiring only certain types of attachments to be sent between Users can use this option to ensure conformance to this policy.

Settings: ..\Microsoft Office InfoPath 2007\Security

Group Policy Object	Recommended State	Version	Scorability
Allow file types as attachments to forms	Not Configured	2007	Y

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath\Security 3. Ensure that the UnsafeFileTypesRemove SZ does not exist.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office InfoPath 2007\Security 3. Double-Click Allow file types as attachments to forms. 4. Select Not Configured, click OK.

Additional References
CCE-1259-1

2.2.1.13. Block Specific File Types As Attachments to Forms

Description
This setting controls which file types (determined by file extension) should be restricted from being added to InfoPath forms as attachments.

Rationale
This setting is informational. Enterprises with a policy requiring only certain types of attachments to be sent between Users can use this option to ensure conformance to this policy.

Settings: ..\Microsoft Office InfoPath 2007\Security			
Group Policy Object	**Recommended State**	**Version**	**Scorability**
Block specific file types as attachments to forms	Not Configured	2007	Y

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath\Security 3. Ensure that the UnsafeFileTypesAdd SZ does not exist.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office InfoPath 2007\Security 3. Double-Click Block specific file types as attachments to forms. 4. Select Not Configured, click OK.

Additional References
CCE-1267-4

2.2.1.14. File Type Restriction from InfoPath Forms as Attachments

Description
This setting controls which file types (determined by file extension) should be restricted from being added to InfoPath forms as attachments.

Rationale
This setting is informational. Enterprises with a policy requiring only certain types of attachments to be sent between Users can use this option to ensure conformance to this policy.

Settings: ..\Microsoft Office InfoPath 2007\Security			
Group Policy Object	**Recommended State**	**Version**	**Scorability**
Prevent Users from allowing unsafe file types to be attached to forms	Enabled	2007	Y

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\InfoPath\Security 3. Ensure that the UnsafeFileTypesAdd DWORD exists and is set to 1.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office InfoPath 2007\Security 3. Double-Click Prevent Users from allowing unsafe file types to be attached to forms. 4. Select Enabled, click OK.

Additional References
CCE-1060-3

2.2.1.15. Block Opening of Text File Types

Description
The **Block opening of Text file types** option determines if Word opens Text files.

Rationale
Setting this option to **Not Configured** marginally lessens the attack surface area of the application.

Settings: ..\Microsoft Office Word 2007\Block file formats\Open			
Group Policy Object	**Recommended State**	**Version**	**Scorability**
Block opening of Text file types	Not Configured	2007	Y

Audit
1. Click Start, click Run, type regedit, and then click OK. 2. Locate and select: HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\Word\Security\FileOpenBlock 3. Ensure that the TextFiles DWORD does not exist.

Remediation
1. Click Start, click Run, type gpedit.msc, and then click OK. 2. Locate and select: User Configuration\Administrative Templates\ Microsoft Office Word 2007\Block file formats\Open 3. Double-Click Block opening of Text file types. 4. Select Not Configured, click OK.

Additional References
CCE-1072-8

2.2.1.16. Disable all Application Add-Ins

Description
The **Disable all application add-ins** setting determines if application add-ins are initialized.

Rationale
Application add-ins could potentially be used by a malicious User to gain code execution on a User's box. Setting this option to **Not Configured** will disable all application add-ins.

Settings: ..\Microsoft Office PowerPoint 2007\PowerPoint Options\Security\Trust

Center			
Group Policy Object	**Recommended State**	**Version**	**Scorability**
Disable all application add-ins	Not Configured	2007	Y

Audit

1. Click Start, click Run, type regedit, and then click OK.
2. Locate and select:
   HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\12.0\PowerPoint\Security
3. Ensure that the DisableAllAddins DWORD does not exist.

Remediation

1. Click Start, click Run, type gpedit.msc, and then click OK.
2. Locate and select:
   User Configuration\Administrative Templates\
   Microsoft Office PowerPoint 2007\PowerPoint Options\Security\Trust Center
3. Double-Click Disable all application add-ins.
4. Select Not Configured, click OK.

Additional References

CCE-1204-7

Appendix A: References

1. 2007 Microsoft Office Security Guide
   http://www.microsoft.com/downloads/details.aspx?FamilyID=a12eca33-a20d-45e2-895c-5e021f3ae4c5&displaylang=en

2. 2007 Microsoft Office Threats and Countermeasures
   http://technet.microsoft.com/en-us/library/cc148226.aspx

3. Security policies and settings in the 2007 Office system
   http://technet.microsoft.com/en-us/library/cc178946.aspx

4. Microsoft Office 2007 Resource Kit
   http://support.microsoft.com/kb/924617

Appendix B: Change History

Date	Version	Changes for this version
December 12, 2009	1.0	Public Release