CIS Microsoft PowerPoint 2013 Benchmark

v1.0.0 - 08-20-2015

The CIS Security Benchmarks division provides consensus-oriented information security products, services, tools, metrics, suggestions, and recommendations (the "SB Products") as a public service to Internet users worldwide. Downloading or using SB Products in any way signifies and confirms your acceptance of and your binding agreement to these CIS Security Benchmarks Terms of Use.

CIS SECURITY BENCHMARKS TERMS OF USE

BOTH CIS SECURITY BENCHMARKS DIVISION MEMBERS AND NON-MEMBERS MAY:

- Download, install, and use each of the SB Products on a single computer, and/or
- Print one or more copies of any SB Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, but only if each such copy is printed in its entirety and is kept intact, including without limitation the text of these CIS Security Benchmarks Terms of Use.

UNDER THE FOLLOWING TERMS AND CONDITIONS:

- **SB Products Provided As Is**. CIS is providing the SB Products "as is" and "as available" without: (1) any representations, warranties, or covenants of any kind whatsoever (including the absence of any warranty regarding: (a) the effect or lack of effect of any SB Product on the operation or the security of any network, system, software, hardware, or any component of any of them, and (b) the accuracy, utility, reliability, timeliness, or completeness of any SB Product); or (2) the responsibility to make or notify you of any corrections, updates, upgrades, or fixes.
- **Intellectual Property and Rights Reserved**. You are not acquiring any title or ownership rights in or to any SB Product, and full title and all ownership rights to the SB Products remain the exclusive property of CIS. All rights to the SB Products not expressly granted in these Terms of Use are hereby reserved.
- **Restrictions**. You acknowledge and agree that you may not: (1) decompile, dis-assemble, alter, reverse engineer, or otherwise attempt to derive the source code for any software SB Product that is not already in the form of source code; (2) distribute, redistribute, sell, rent, lease, sublicense or otherwise transfer or exploit any rights to any SB Product in any way or for any purpose; (3) post any SB Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device; (4) remove from or alter these CIS Security Benchmarks Terms of Use on any SB Product; (5) remove or alter any proprietary notices on any SB Product; (6) use any SB Product or any component of an SB Product with any derivative works based directly on an SB Product or any component of an SB Product; (7) use any SB Product or any component of an SB Product with other products or applications that are directly and specifically dependent on such SB Product or any component for any part of their functionality; (8) represent or claim a particular level of compliance or consistency with any SB Product; or (9) facilitate or otherwise aid other individuals or entities in violating these CIS Security Benchmarks Terms of Use.
- **Your Responsibility to Evaluate Risks**. You acknowledge and agree that: (1) no network, system, device, hardware, software, or component can be made fully secure; (2) you have the sole responsibility to evaluate the risks and benefits of the SB Products to your particular circumstances and requirements; and (3) CIS is not assuming any of the liabilities associated with your use of any or all of the SB Products.
- **CIS Liability**. You acknowledge and agree that neither CIS nor any of its employees, officers, directors, agents or other service providers has or will have any liability to you whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages that arise out of or are connected in any way with your use of any SB Product.
- **Indemnification**. You agree to indemnify, defend, and hold CIS and all of CIS's employees, officers, directors, agents and other service providers harmless from and against any liabilities, costs and expenses incurred by any of them in connection with your violation of these CIS Security Benchmarks Terms of Use.
- **Jurisdiction**. You acknowledge and agree that: (1) these CIS Security Benchmarks Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland; (2) any action at law or in equity arising out of or relating to these CIS Security Benchmarks Terms of Use shall be filed only in the courts located in the State of Maryland; and (3) you hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action.
- **U.S. Export Control and Sanctions laws**. Regarding your use of the SB Products with any non-U.S. entity or country, you acknowledge that it is your responsibility to understand and abide by all U.S. sanctions and export control laws as set from time to time by the U.S. Bureau of Industry and Security (BIS) and the U.S. Office of Foreign Assets Control (OFAC).

SPECIAL RULES FOR CIS MEMBER ORGANIZATIONS: CIS reserves the right to create special rules for: (1) CIS Members; and (2) Non-Member organizations and individuals with which CIS has a written contractual relationship. CIS hereby grants to each CIS Member Organization in good standing the right to distribute the SB Products within such Member's own organization, whether by manual or electronic means. Each such Member Organization acknowledges and agrees that the foregoing grants in this paragraph are subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Table of Contents

Overview

This document, Security Configuration Benchmark for Microsoft PowerPoint 2013, provides prescriptive guidance for establishing a secure configuration posture for Microsoft PowerPoint 2013 running on Windows 7. This guide was tested against Microsoft Office 2013. 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.

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 PowerPoint 2013 on a Microsoft Windows platform.

Consensus Guidance

This benchmark was created using a consensus review process comprised 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 published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the benchmark. If you are interested in participating in the consensus process, please visit https://community.cisecurity.org.

Typographical 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

Scoring Information

A scoring status indicates whether compliance with the given recommendation impacts the assessed target's benchmark score. The following scoring statuses are used in this benchmark:

Scored

Failure to comply with "Scored" recommendations will decrease the final benchmark score. Compliance with "Scored" recommendations will increase the final benchmark score.

Not Scored

Failure to comply with "Not Scored" recommendations will not decrease the final benchmark score. Compliance with "Not Scored" recommendations will not increase the final benchmark score.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

    Items in this profile intend to:

    - Be practical and prudent;
    - Provide a clear security benefit; and
    - Not inhibit the utility of the technology beyond acceptable means.

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:

Contributor
Hardeep Mehrotara CISSP, CISA, GSEC, ISMSA

Editor
Jordan Rakoske GSEC
Edward Oechsner GSEC

Recommendations

1 User Configuration

1.1 Miscellaneous

1.1.1 Set 'Disable Slide Update' to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether users can link slides in a presentation with their counterparts in a PowerPoint Slide Library.

If you enable this policy setting, PowerPoint cannot check the status of a slide in a Slide Library when a presentation with Slide Update data is opened.

If you disable or do not configure this policy setting, each time users open a presentation that contains a shared slide, PowerPoint notifies them if the slide has been updated and provides them with the opportunity to ignore the update, append a new slide to the outdated slide, or replace the outdated slide with the updated one. The recommended state for this setting is: `Enabled`.

Rationale:

PowerPoint 2013 users can share and reuse slide content by storing individual slide files in a centrally located Slide Library on a server running Office SharePoint Server 2013. Using the Slide Update feature, users can associate a slide in a presentation on a user's computer with the original slide that resides in the Slide Library on the server.

By default, each time users open a presentation that contains a shared slide, PowerPoint 2013 notifies them if the slide has been updated and provides them with the opportunity to ignore the update, append a new slide to the outdated slide, or replace the outdated slide with the updated one. In some situations, updating a slide in a presentation from an external source like a Slide Library can cause important information to be lost. An attacker

could modify the data in the slide library, affecting the integrity of all slide presentations that depend upon that library.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\slide
libraries\disableslideupdate
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint
2013\Miscellaneous\Disable Slide Update
```

Impact:

Enabling this setting prevents PowerPoint 2013 from checking Slide Libraries for slide updates. Users who work with slides associated with Slide Libraries will have to use some other mechanism to update slides in their presentations. Users who do not work with Slide Libraries will not be affected by this setting.

Default Value:

Not Configured

References:

1. CCE-29267-2

1.2 PowerPoint Options

1.2.1 Set 'Default file format' to Enabled (PowerPoint Presentation (*pptx)) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting governs the default format for new presentation files that users create.

If you enable this policy setting, when a user creates a new blank presentation, it is in the specified default format. Users may still override the default and specify a specific format when they create a presentation.

If you disable or do not configure this policy setting, PowerPoint Presentation is the default option. The recommended state for this setting is: `Enabled`. `(PowerPoint Presentation (*pptx))`

Rationale:

By default, when users create new PowerPoint files, PowerPoint 2013 saves them in the new *.pptx file format. Users can change this functionality by clicking the Office button, clicking PowerPoint Options, and then selecting a file format from the Default file format list.

Disabling this setting allows users to choose from any of the available default file formats. If a new PowerPoint file is created in an earlier format, some users may not be unable to open or use the file, or they may choose a format that is less secure than the PowerPoint 2013 format.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\options\defaultfor
mat
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint
Options\Save\Default file format
```

Impact:

Enabling this setting does not prevent users from choosing a different file format for a new PowerPoint file, and therefore, it is unlikely to affect usability for most users.

Default Value:

Not Configured

References:

1. CCE-29303-5

1.2.2 Set 'Make Hidden Markup Visible' to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether hidden markup is visible when users open PowerPoint files in standard or HTML format.

If you enable this policy setting, PowerPoint ignores this flag when opening a file, and always displays any markup present in the file. In addition, when saving a file, PowerPoint sets the flag to display markup when the presentation is next opened.

If you disable this policy setting, PowerPoint sets the flag according to the state of the "Show Markup" option on the Review tab of the Ribbon when it saves presentations in standard or HTML format. In addition, PowerPoint enables or disables the "Show Markup" option according to the way the flag is set when it opens files, which means that a presentation saved with hidden markup is opened with the markup still hidden.

If you disable this policy setting, the behavior is the equivalent of Enabled. The recommended state for this setting is: `Enabled`.

Rationale:

PowerPoint presentations that are saved in standard or HTML format can contain a flag indicating whether markup (comments or ink annotations) in the presentation should be visible when the presentation is open. By default, PowerPoint 2013 ignores this flag when opening a file, and always displays any markup present in the file. In addition, when saving a file, PowerPoint sets the flag to display markup when the presentation is next opened.

If this default configuration is changed, PowerPoint sets the flag according to the state of the Show Markup option on the Review tab of the Ribbon when it saves presentations in standard or HTML format. In addition, PowerPoint enables or disables the Show Markup option according to the way the flag is set when it opens files, which means that a presentation saved with hidden markup is opened with the markup still hidden.

If a file is saved with hidden markup, users might inadvertently distribute sensitive comments or information to others via the presentation file.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\options\markupopen
save
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint
Options\Security\Make Hidden Markup Visible
```

Impact:

If this setting is Enabled, hidden markup will be visible when the file is opened, and if users intend it to be hidden they will need to hide it again. (Users can permanently locate and remove undesired markup from files by using the Document Inspector feature in PowerPoint 2013.) Enabling this setting enforces the default configuration in PowerPoint 2013.

In most cases, markup is intended to be visible to users. Markup does not display in presentation mode in PowerPoint, even if it is visible in design mode, so it is likely that this setting will have a minimal impact on usability.

Default Value:

Not Configured

References:

1. CCE-29364-7

1.2.3 Set 'Scan Encrypted Macros in PowerPoint Open XML Presentations' to Enabled (Scan Encrypted Macros) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether encrypted macros in Open XML presentations are required to be scanned with anti-virus software before being opened.

If you enable this policy setting, you may choose one of these options:

- Scan encrypted macros: encrypted macros are disabled unless anti-virus software is installed. Encrypted macros are scanned by your anti-virus software when you attempt to open an encrypted presentation that contains macros.

- Scan if anti-virus software available: if anti-virus software is installed, scan the encrypted macros first before allowing them to load. If anti-virus software is not available, allow encrypted macros to load.

- Load macros without scanning: do not check for anti-virus software and allow macros to be loaded in an encrypted file.

If you disable or do not configure this policy setting, the behavior will be similar to the "Scan encrypted macros" option. The recommended state for this setting is: `Enabled`. `(Scan Encrypted Macros)`

Rationale:

When an Office Open XML presentation is rights-managed or password-protected, any macros that are embedded in the presentation are encrypted along with the rest of the workbook's contents. By default, these encrypted macros will be disabled unless they are scanned by antivirus software immediately before being loaded.

If this setting is Disabled, PowerPoint 2013 will not require encrypted macros to be scanned before loading. PowerPoint will handle them as specified by the Office 2013 System macro security settings, which can cause macro viruses to load undetected and lead to data loss or reduced application functionality.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\powerpoin
tbypassencryptedmacroscan
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint
Options\Security\Scan Encrypted Macros in PowerPoint Open XML Presentations
```

Impact:

Enabling this setting enforces the default configuration in PowerPoint 2013, and is therefore unlikely to cause usability issues for most users.

Default Value:

Not Configured

References:

1. CCE-29362-1

1.2.4 Set 'Run Programs' to Enabled (Disable (Don't Run Any Programs)) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls the prompting and activation behavior for the "Run Programs" option for action buttons in PowerPoint.

If you enable this policy setting, you can choose from three options to control how the "Run Programs" option functions:

- Disable (don't run any programs). If users click an action button with the "Run Programs" action assigned to it, nothing will happen. This option enforces the default configuration in PowerPoint.

- Enable (prompt user before running). If users click an action button with the "Run Programs" action assigned to it, PowerPoint will prompt them to continue before running the program.

- Enable all (run without prompting). If users click an action button with the "Run Programs" action assigned to it. PowerPoint will run the program automatically, without prompting.

If you disable or do not configure this policy setting, if users click an action with the "Run Programs" action assigned to it, nothing will happen. This behavior is the same as Enabled - - Disable (don't run any programs).

The recommended state for this setting is: `Enabled.  (Disable (Don't Run Any Programs))`

Rationale:

Action buttons can be used to launch external programs from PowerPoint 2013 presentations. If a malicious person adds an action button to a presentation that launches a dangerous program, it could significantly affect the security of a user's computer and data.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\runprograms
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint
Options\Security\Run Programs
```

Impact:

Enabling this setting and configuring the drop-down menu to "Disable (don't run any programs)" will cause disruptions to users who wish to create or use presentations that launch external programs when action buttons are clicked. These users will have to launch any external programs manually at the appropriate times when delivering presentations.

Default Value:

Not Configured

References:

1. CCE-29365-4

1.2.5 Set 'Turn Off File Validation' to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you turn off the file validation feature.

If you enable this policy setting, file validation will be turned off.

If you disable or do not configure this policy setting, file validation will be turned on. Office Binary Documents (97-2003) are checked to see if they conform against the file format schema before they are opened. The recommended state for this setting is: `Disabled`.

Rationale:

The file validation feature ensures that Office Binary Documents are checked to see if they conform against the file format schema before they are opened, which may help protect against certain types of attacks.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\filevalid
ation\enableonload
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint
Options\Security\Turn Off File Validation
```

Impact:

If you enable this policy setting, file validation will be turned off. If you disable or do not configure this policy setting, file validation will be turned on. Office Binary Documents (97-2003) are checked to see if they conform against the file format schema before they are opened.

Default Value:

Not Configured

References:

1. CCE-29366-2

1.2.6 Set 'Unblock Automatic Download of Linked Images' to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting determines whether PowerPoint automatically downloads links from external sources.

If you enable this policy setting, PowerPoint will load images saved in remote locations.

If you disable or do not configure this policy setting, when PowerPoint opens a presentation it does not display any linked images saved on a different computer unless the presentation itself is saved in a trusted location (as configured in the Trust Center). The recommended state for this setting is: `Disabled`.

Rationale:

When users insert images into PowerPoint 2013 presentations, they can select Link to File instead of Insert. If they do so, the image is represented by a link to a file on disk instead of being embedded in the presentation file itself.

By default, when PowerPoint opens a presentation it does not display any linked images saved on a different computer unless the presentation itself is saved in a trusted location (as configured in the Trust Center). If this configuration is changed, PowerPoint will load any images that were saved in remote locations, which presents a security risk.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\downloadi
mages
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint
Options\Security\Unblock Automatic Download of Linked Images
```

Impact:

Disabling this setting enforces the default configuration of PowerPoint 2013, and is therefore unlikely to cause significant usability issues for most users.

Default Value:

Not Configured

References:

1. CCE-29363-9

1.2.7 Set 'Disable Trust Bar Notification for Unsigned Application Add-ins and Block Them' to Enable (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether the specified Office application notifies users when unsigned application add-ins are loaded or silently disable such add-ins without notification. This policy setting only applies if you enable the "Require that application add-ins are signed by Trusted Publisher" policy setting, which prevents users from changing this policy setting.

If you enable this policy setting, applications automatically disable unsigned add-ins without informing users.

If you disable this policy setting, if this application is configured to require that all add-ins be signed by a trusted publisher, any unsigned add-ins the application loads will be disabled and the application will display the Trust Bar at the top of the active window. The Trust Bar contains a message that informs users about the unsigned add-in.

If you do not configure this policy setting, the disable behavior applies, and in addition, users can configure this requirement themselves in the "Add-ins" category of the Trust Center for the application. The recommended state for this setting is: `Enabled`.

Rationale:

By default, if an application is configured to require that all add-ins be signed by a trusted publisher, any unsigned add-ins the application loads will be disabled and the application will display the Trust Bar at the top of the active window. The Trust Bar contains a message that informs users about the unsigned add-in.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\notbpromp
tunsignedaddin
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint
Options\Security\Trust Center\Disable Trust Bar Notification for Unsigned Application
Add-ins and Block Them
```

Impact:

This setting only applies if the Office 2013 application is configured to require that all add-ins are signed by a trusted publisher. By default, users can configure this requirement themselves in the Add-ins category of the Trust Center for the application. To enforce this requirement, you must enable the Require that application add-ins are signed by Trusted Publisher setting in Group Policy, which prevents users from changing the setting themselves.

Default Value:

Not Configured

References:

1. CCE-29354-8

1.2.8 Set 'Trust Access to Visual Basic Project' to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether automation clients such as Microsoft Visual Studio 2005 Tools for Microsoft Office (VSTO) can access the Visual Basic for Applications project system in the specified applications. VSTO projects require access to the Visual Basic for Applications project system in Excel, PowerPoint, and Word, even though the projects do not use Visual Basic for Applications. Design-time support of controls in both Visual Basic and C# projects depends on the Visual Basic for Applications project system in Word and Excel.

If you enable this policy setting, VSTO and other automation clients can access the Visual Basic for Applications project system in the specified applications. Users will not be able to change this behavior through the "Trust access to the VBA project object model" user interface option under the Macro Settings section of the Trust Center.

If you disable this policy setting, VSTO does not have programmatic access to VBA projects. In addition, the "Trust access to the VBA project object model" check box is cleared and users cannot change it. Note: Disabling this policy setting prevents VSTO projects from interacting properly with the VBA project system in the selected application.

If you do not configure this policy setting, automation clients do not have programmatic access to VBA projects. Users can enable this by selecting the "Trust access to the VBA project object model" in the "Macro Settings" section of the Trust Center. However, doing so allows macros in any documents the user opens to access the core Visual Basic objects, methods, and properties, which represents a potential security hazard.

The recommended state for this setting is: `Disabled`.

Rationale:

VSTO projects require access to the Visual Basic for Applications project system in Excel 2013, PowerPoint 2013, and Word 2013, even though the projects do not use Visual Basic for Applications. Design-time support of controls in both Visual Basic and C# projects depends on the Visual Basic for Applications project system in Word and Excel.

By default, Excel, Word, and PowerPoint do not allow automation clients to have programmatic access to VBA projects. Users can enable this by selecting the Trust access to

the VBA project object model in the Macro Settings section of the Trust Center. However, doing so allows macros in any documents the user opens to access the core Visual Basic objects, methods, and properties, which represents a potential security hazard.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\accessvbo
m
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to

`Disabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint
Options\Security\Trust Center\Trust Access to Visual Basic Project
```

Impact:

Disabling this setting enforces the default configuration in Excel 2013, Word 2013, and PowerPoint 2013 and is therefore unlikely to cause significant usability issues for most users.

Default Value:

Not Configured

References:

1. CCE-29358-9

1.2.9 Set 'Require That Application Add-ins are Signed by Trusted Publisher' to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether add-ins for this applications must be digitally signed by a trusted publisher.

If you enable this policy setting, this application checks the digital signature for each add-in before loading it. If an add-in does not have a digital signature, or if the signature did not come from a trusted publisher, this application disables the add-in and notifies the user. Microsoft provides four certificates for Office, which you can add to the Trusted Publishers list. These certificates must be added to the Trusted Publishers list if you require that all add-ins be signed by a trusted publisher. The Microsoft certificates are named Mscert01.cer, Mscert02.cer, Mscert03.cer, Mscert04.cer, and can be found on the Microsoft Web site. Office 2013 stores certificates for trusted publishers in the Internet Explorer trusted publisher store. Earlier versions of Microsoft Office stored trusted publisher certificate information (specifically, the certificate thumbprint) in a special Office trusted publisher store. Office 2013 still reads trusted publisher certificate information from the Office trusted publisher store, but it does not write information to this store. Therefore, if you created a list of trusted publishers in a previous version of Office and you upgrade to Office 2013, your trusted publisher list will still be recognized. However, any trusted publisher certificates that you add to the list will be stored in the Internet Explorer trusted publisher store. For more information about trusted publishers, see the Office Resource Kit.

If you disable or do not configure this policy setting, this application does not check the digital signature on application add-ins before opening them. If a dangerous add-in is loaded, it could harm users' computers or compromise data security. The recommended state for this setting is: `Enabled`.

Rationale:

By default, Office 2013 applications do not check the digital signature on application add-ins before opening them. Disabling or not configuring this setting may allow an application to load a dangerous add-in. As a result, malicious code could become active on user computers or the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\requiread
dinsig
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint
Options\Security\Trust Center\Require That Application Add-ins are Signed by Trusted
Publisher
```

Impact:

Enabling this setting could cause disruptions for users who rely on add-ins that are not signed by trusted publishers. These users will either have to obtain signed versions of such add-ins or stop using them.

Office 2013 stores certificates for trusted publishers in the Internet Explorer trusted publisher store. Earlier versions of Office stored trusted publisher certificate information (specifically, the certificate thumbprint) in a special Office trusted publisher store. Office 2013 still reads trusted publisher certificate information from the Office trusted publisher store, but does not write information to this store.

Therefore, if you created a list of trusted publishers in a previous version of Office and you upgrade to the Office 2013 release, your trusted publisher list will still be recognized. However, any trusted publisher certificates that you add to the list will be stored in the Internet Explorer trusted publisher store.

Default Value:

Not Configured

References:

1. CCE-29355-5

1.2.10 Set 'VBA Macro Notification Settings' to Enabled (Disable all Except Digitally Signed) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls how the specified applications warn users when Visual Basic for Applications (VBA) macros are present.

If you enable this policy setting, you can choose from four options for determining how the specified applications will warn the user about macros:

- Disable all with notification: The application displays the Trust Bar for all macros, whether signed or unsigned. This option enforces the default configuration in Office.

- Disable all except digitally signed macros: The application displays the Trust Bar for digitally signed macros, allowing users to enable them or leave them disabled. Any unsigned macros are disabled, and users are not notified.

- Disable all without notification: The application disables all macros, whether signed or unsigned, and does not notify users.

- Enable all macros (not recommended): All macros are enabled, whether signed or unsigned. This option can significantly reduce security by allowing dangerous code to run undetected.

If you disable this policy setting, "Disable all with notification" will be the default setting.

If you do not configure this policy setting, when users open files in the specified applications that contain VBA macros, the applications open the files with the macros disabled and display the Trust Bar with a warning that macros are present and have been disabled. Users can inspect and edit the files if appropriate, but cannot use any disabled functionality until they enable it by clicking "Enable Content" on the Trust Bar. If the user clicks "Enable Content", then the document is added as a trusted document.

Important: If "Disable all except digitally signed macros" is selected, users will not be able to open unsigned Access databases.

Also, note that Microsoft Office stores certificates for trusted publishers in the Internet Explorer trusted publisher store. Earlier versions of Microsoft Office stored trusted publisher certificate information (specifically, the certificate thumbprint) in a special Office trusted publisher store. Microsoft Office still reads trusted publisher certificate information from the Office trusted publisher store, but it does not write information to this store.

Therefore, if you created a list of trusted publishers in a previous version of Microsoft Office and you upgrade to Office, your trusted publisher list will still be recognized. However, any trusted publisher certificates that you add to the list will be stored in the

Internet Explorer trusted publisher store.   The recommended state for this setting is: `Enabled`.

Rationale:

By default, when users open files in PowerPoint 2013 that contain VBA macros, PowerPoint 2013 opens the files with the macros disabled, and displays the Trust Bar with a warning that macros are present and have been disabled. Users may then enable these macros by clicking Options on the Trust Bar and selecting the option to enable them.

Disabling or not configuring this setting may allow dangerous macros to become active on user computers or the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\vbawarnin
gs
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint
Options\Security\Trust Center\VBA Macro Notification Settings
```

Impact:

This configuration causes documents and templates that contain unsigned macros to lose any functionality supplied by those macros. To prevent this loss of functionality, users can install the macros in a trusted location, unless the Disable all trusted locations setting is configured to Enabled, which will block them from doing so. If your organization does not use any officially sanctioned macros, consider choosing No Warnings for all macros but disable all macros for even stronger security.

Default Value:

Not Configured

References:

1. CCE-29361-3

1.2.11 Set 'Default File Block Behavior' to Enabled (Blocked files are not opened) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to determine if users can open, view, or edit Word files.

If you enable this policy setting, you can set one of these options:

- Blocked files are not opened

- Blocked files open in Protected View and cannot be edited

- Blocked files open in Protected View and can be edited

If you disable or do not configure this policy setting, the behavior is the same as the "Blocked files are not opened" setting. Users will not be able to open blocked files. The recommended state for this setting is: `Enabled. (Blocked files are not opened)`

Rationale:

By default, users can open, view, or edit a large number of file types in PowerPoint 2013. Some file types are safer than others, as some could allow malicious code to become active on user computers or the network. For this reason, disabling or not configuring this setting could allow malicious code to become active on user computers or the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\fileblock
\openinprotectedview
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint
Options\Security\Trust Center\File Block Settings\Default File Block Behavior
```

Impact:

Enabling this setting prevents users from opening, viewing, or editing certain types of files in PowerPoint 2013. Productivity in your organization could be affected if users who require access to any of these file types cannot access them.

Default Value:

Not Configured

References:

1. CCE-29324-1

1.2.12 Set ' Document Behavior if File Validation Fails' to Enabled (Open in Protected View (Unchecked)) (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls how Office handles documents when they fail file validation.

If you enable this policy setting, you can configure the following options for files that fail file validation:

- Block files completely. Users cannot open the files.

- Open files in Protected View and disallow edit. Users cannot edit the files. This is also how Office handles the files if you disable this policy setting.

- Open files in Protected View and allow edit. Users can edit the files. This is also how Office handles the files if you do not configure this policy setting.

If you disable this policy setting, Office follows the "Open files in Protected View and disallow edit" behavior.

If you do not configure this policy setting, Office follows the "Open files in Protected View and allow edit" behavior. The recommended state for this setting is: `Enabled`. (`Open in Protected View (Unchecked)`)

Rationale:

Disabling or not configuring this setting allows users to open and edit files that have failed file validation outside of Protected View. As a result, malicious code or users could become active on user computers or the network. For example, a malicious user may purposely put invalid data in a file. The invalid data could force the program to fail or execute its code in an unexpected manner, giving the malicious user control of the application.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\filevalid
ation\disableeditfrompv
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\filevalid
ation\openinprotectedview
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint
Options\Security\Trust Center\Protected View\Set Document Behavior if File Validation
Fails
```

Impact:

By default, users can only open files in Protected View after the files fail validation to help prevent malicious code from running on user computers or the network. In this way, the application is protected from attacks attempting to induce unexpected execution paths. You can block files from opening at all, but this also prevents users from accessing any data in the file.

Using this setting allows the application to open files, and thus users to view valid data and detect invalid data that is visible. However, users cannot correct invalid data in the file. To do so, users must open such files on another isolated computer where this setting is set to a lower security level.

Default Value:

Not Configured

References:

1. CCE-29329-0

1.2.13 Set 'Do not open from the Internet zone in Protected View' to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to determine if files downloaded from the Internet zone open in Protected View.

If you enable this policy setting, files downloaded from the Internet zone do not open in Protected View.

If you disable or do not configure this policy setting, files downloaded from the Internet zone open in Protected View. The recommended state for this setting is: `Disabled`.

Rationale:

Enabling this setting allows files that users download from the Internet zone open outside of Protected View. This could allow malicious code to become active on user computers or the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\protected
view\disableinternetfilesinpv
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to Disabled.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint
Options\Security\Trust Center\Protected View\Do not open files from the Internet zone
in Protected View
```

Impact:

When files open in Protected View, some functionality will be unavailable and productivity in your organization could be affected. When this is undesirable, users will have to add

sites to their trusted sites list in Internet Explorer, thus allowing the files to be opened in normal view with all functionality available.

Default Value:

Not Configured

References:

1. CCE-29326-6

1.2.14 Set 'Turn off Protected View for attachments opened from Outlook' to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows you to determine if PowerPoint files in Outlook attachments open in Protected View.

If you enable this policy setting, Outlook attachments do not open in Protected View.

If you disable or do not configure this policy setting, Outlook attachments open in Protected View. The recommended state for this setting is: `Disabled`.

Rationale:

Enabling this setting allows Outlook 2013 attachments to open outside of Protected View. Email is a common way to spread files containing malicious code. This could allow malicious code to become active on user computers or the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\protected
view\disableattachmentsinpv
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint
Options\Security\Trust Center\Protected View\Turn off Protected View for attachments
opened from Outlook
```

Impact:

Opening Office 2013 files, such as the Office 2013 versions of Word, Excel, PowerPoint, and OneNote, is a common action. Users are unlikely to notice much difference when opening and viewing files in Protected View. Users who want to modify these kinds of files must save them to a safe location and then open them.

When Office 2013 application files open in Protected View, some functionality is unavailable. The process of dragging the file to a new location and then opening it takes more time than simply double-clicking the file to open it, modifying it, and then saving it to the same location. For these reasons, administrators may receive some complaints from users potentially confused about how to modify files originally only available to them in Protected View.

Default Value:

Not Configured

References:

1. CCE-29330-8

1.2.15 Set 'Do not open files in unsafe locations in Protected View' to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting lets you determine if files located in unsafe locations will open in Protected View. If you have not specified unsafe locations, only the "Downloaded Program Files" and "Temporary Internet Files" folders are considered unsafe locations.

If you enable this policy setting, files located in unsafe locations do not open in Protected View.

If you disable or do not configure this policy setting, files located in unsafe locations open in Protected View. The recommended state for this setting is: `Disabled`.

Rationale:

Enabling this setting allows users to open files located in unsafe locations that do not require Protected View. As a result, malicious code could become active on user computers or the network.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\protected
view\disableunsafelocationsinpv
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint
Options\Security\Trust Center\Protected View\Do not open files in unsafe locations in
Protected View
```

Impact:

The Downloaded Program Files folder and the Temporary Internet Files folder are considered unsafe locations. You may specify additional unsafe locations.

Some functionality is not available when files are opened in Protected View. In such cases, users must move the files from unsafe locations to save locations in order to access them with full functionality

Default Value:

Not Configured

References:

1. CCE-29327-4

1.2.16 Set 'Allow Trusted Locations on the network' to Disabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting controls whether trusted locations on the network can be used.

If you enable this policy setting, users can specify trusted locations on network shares or in other remote locations that are not under their direct control by clicking the "Add new location" button in the Trusted Locations section of the Trust Center. Content, code, and add-ins are allowed to load from trusted locations with minimal security and without prompting the user for permission.

If you disable this policy setting, the selected application ignores any network locations listed in the Trusted Locations section of the Trust Center.

If you also deploy Trusted Locations via Group Policy, you should verify whether any of them are remote locations. If any of them are remote locations and you do not allow remote locations via this policy setting, those policy keys that point to remote locations will be ignored on client computers.

Disabling this policy setting does not delete any network locations from the Trusted Locations list, but causes disruption for users who add network locations to the Trusted Locations list. Users are also prevented from adding new network locations to the Trusted Locations list in the Trust Center. We recommended that you do not enable this policy setting (as the "Allow Trusted Locations on my network (not recommended)" check box also states). Therefore, in practice, it should be possible to disable this policy setting in most situations without causing significant usability issues for most users.

If you do not enable this policy setting, users can select the "Allow Trusted Locations on my network (not recommended)" check box if desired and then specify trusted locations by clicking the "Add new location" button. The recommended state for this setting is: `Disabled`.

Rationale:

By default, files located in trusted locations and specified in the Trust Center are assumed to be safe. Content, code, and add-ins are allowed to load from trusted locations with minimal security and without prompting the user for permission.

By default, users can specify trusted locations on network shares or in other remote locations that are not under their direct control by selecting the Allow Trusted Locations on my network (not recommended) check box in the Trusted Locations section of the Trust Center. If a dangerous file is opened from a trusted location, it will not be subject to typical security measures and could affect users' computers or data.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\trusted
locations\allownetworklocations
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Disabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint
Options\Security\Trust Center\Trusted Locations\Allow Trusted Locations on the network
```

Impact:

Disabling this setting will cause disruption for users who add network locations to the Trusted Locations list. However, this practice is discouraged (as the Allow Trusted Locations on my network (not recommended) check box itself states), so in practice it should be possible to disable this setting in most situations without causing significant usability issues for most users.

Default Value:

Not Configured

References:

1. CCE-29331-6

1.2.17 Set 'Disable all trusted locations' to Enabled (Scored)

Profile Applicability:

- Level 1

Description:

This policy setting allows administrators to disable all trusted locations in the specified applications. Trusted locations specified in the Trust Center are used to define file locations that are assumed to be safe. Content, code, and add-ins are allowed to load from trusted locations with a minimal amount of security, without prompting the users for permission. If a dangerous file is opened from a trusted location, it will not be subject to standard security measures and could harm users' computers or data.

If you enable this policy setting, all trusted locations (those specified in the Trust Center) in the specified applications are ignored, including any trusted locations established by Office 2013 during setup, deployed to users using Group Policy, or added by users themselves. Users will be prompted again when opening files from trusted locations.

If you disable or do not configure this policy setting, all trusted locations (those specified in the Trust Center) in the specified applications are assumed to be safe. The recommended state for this setting is: `Enabled`.

Rationale:

Trusted locations specified in the Trust Center are used to define file locations that are assumed to be safe. Content, code, and add-ins are allowed to load from trusted locations with a minimal amount of security, without prompting the users for permission. If a dangerous file is opened from a trusted location, it will not be subject to standard security measures and could harm users' computers or data.

By default, files located in trusted locations (those specified in the Trust Center) are assumed to be safe.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed. This group policy setting is backed by the following registry location:

```
HKEY_USERS\<SID>\software\policies\microsoft\office\15.0\powerpoint\security\trusted
locations\alllocationsdisabled
```

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Enabled`.

```
User Configuration\Administrative Templates\Microsoft PowerPoint 2013\PowerPoint
Options\Security\Trust Center\Trusted Locations\Disable all trusted locations
```

Impact:

If there are business-critical reasons to access some files in a more trusted environment, disabling trusted locations could cause usability problems.

Default Value:

Not Configured

References:

1. CCE-29332-4

Control		Set Correctly	
		Yes	No
1	**User Configuration**		
1.1	**Miscellaneous**		
1.1.1	Set 'Disable Slide Update' to Enabled (Scored)	☐	☐
1.2	**PowerPoint Options**		
1.2.1	Set 'Default file format' to Enabled (PowerPoint Presentation (*pptx)) (Scored)	☐	☐
1.2.2	Set 'Make Hidden Markup Visible' to Enabled (Scored)	☐	☐
1.2.3	Set 'Scan Encrypted Macros in PowerPoint Open XML Presentations' to Enabled (Scan Encrypted Macros) (Scored)	☐	☐
1.2.4	Set 'Run Programs' to Enabled (Disable (Don't Run Any Programs)) (Scored)	☐	☐
1.2.5	Set 'Turn Off File Validation' to Disabled (Scored)	☐	☐
1.2.6	Set 'Unblock Automatic Download of Linked Images' to Disabled (Scored)	☐	☐
1.2.7	Set 'Disable Trust Bar Notification for Unsigned Application Add-ins and Block Them' to Enable (Scored)	☐	☐
1.2.8	Set 'Trust Access to Visual Basic Project' to Disabled (Scored)	☐	☐
1.2.9	Set 'Require That Application Add-ins are Signed by Trusted Publisher' to Enabled (Scored)	☐	☐

1.2.10	Set 'VBA Macro Notification Settings' to Enabled (Disable all Except Digitally Signed) (Scored)	☐	☐
1.2.11	Set 'Default File Block Behavior' to Enabled (Blocked files are not opened) (Scored)	☐	☐
1.2.12	Set ' Document Behavior if File Validation Fails' to Enabled (Open in Protected View (Unchecked)) (Scored)	☐	☐
1.2.13	Set 'Do not open from the Internet zone in Protected View' to Disabled (Scored)	☐	☐
1.2.14	Set 'Turn off Protected View for attachments opened from Outlook' to Disabled (Scored)	☐	☐
1.2.15	Set 'Do not open files in unsafe locations in Protected View' to Disabled (Scored)	☐	☐
1.2.16	Set 'Allow Trusted Locations on the network' to Disabled (Scored)	☐	☐
1.2.17	Set 'Disable all trusted locations' to Enabled (Scored)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
8/20/15	1.0.0	Initial Release