

UNCLASSIFIED



Desktop Application Antispyware General

Version: 4

Release: 1

03 Dec 2009

STIG.DOD.MIL

Sort Order: [Group ID \(Vulid\), ascending order](#)

Notice: Developed by DISA for the DoD

Description:

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist

Confidential System = CONFIDENTIAL Checklist

Secret System = SECRET Checklist

Top Secret System = SECRET Checklist

Group ID (Vulid): V-14678

Group Title: DTSG001-AntiSpyware software not installed on acce

Rule ID: SV-15354r4_rule

Severity: CAT I

Rule Version (STIG-ID): DTSG001

Rule Title: AntiSpyware software is not installed or not configured for on access and on demand detection.

Vulnerability Discussion: This setting is required for the antispyware software. Without on-access and on-demand scan enabled, the virus scan is not scanning files as they are being accessed.

Responsibility: System Administrator

Check Content:

Procedure: Examine the machine to determine if an Antispyware program is installed. If it is installed, ensure that it is configured for on-access and on-demand detection.

Criteria: If a program is installed and configured for on-access and on-demand detection, this is not a finding.

Please Note: Antispyware products are available on JTF-GNO website for download, such as McAfee Antispyware Enterprise 8.5 and Symantec Antivirus Corporate Edition 10.1 and 10.2 (Vista).

Fix Text: Criteria: Install a program and configured for on-access and on-demand detection.

Please Note: Products are available on JTF-GNO website for download, such as McAfee Antispyware Enterprise 8.5 and Symantec Antivirus Corporate Edition 10.1 and 10.2 (Vista).

Group ID (Vulid): V-14679

Group Title: DTSG002-Antispyware software not at supported leve

Rule ID: SV-15355r2_rule

Severity: CAT I

Rule Version (STIG-ID): DTSG002

Rule Title: The Antispyware software is not at a vendor supported level.

Vulnerability Discussion: This setting is required for the antispyware software. Installed software must be at a vendor supported level.

Responsibility: System Administrator

Check Content:

Procedure: Note the version release level of the antispyware software. This can normally be accomplished by opening the console and clicking on Help, then About.

Criteria: Validate with the vendor's website that this version of the product is on the supported products list. If it is on the list, this is not a finding.

Fix Text: Upgrade to a supported version of the product.

Group ID (Vulid): [V-14680](#)

Group Title: DTSG003-Migration plan does not exist for Antispyw

Rule ID: SV-15356r2_rule

Severity: CAT II

Rule Version (STIG-ID): DTSG003

Rule Title: A migration plan does not exist for Antispyware software that is scheduled to go non-support by the vendor.

Vulnerability Discussion: This setting is required for the antispyware software. A migration plan must be in place for the antispyware that is planned for End-of-Life or the end of vendor support.

Responsibility: System Administrator

Check Content:

Procedure: Note the version release level of the antispyware software. This can normally be accomplished by opening the console and clicking on Help, then About.

Criteria: Determine from the vendor's web site, if the vendor has announced non-support dates for the software. If the vendor has announced a non-support date, ask the IOA for a copy of the migration plan. If a plan exists, this is not a finding. If the product has not been announced as going non-support, this finding is Not Applicable.

Fix Text: Create a migration plan for updating to a supported version of the product prior to its becoming non-supported.

Group ID (Vulid): [V-14682](#)

Group Title: DTSG004-Antispyware software maintenance rollup

Rule ID: SV-15358r2_rule

Severity: CAT II

Rule Version (STIG-ID): DTSG004

Rule Title: The Antispyware software does not have the latest maintenance rollup of software update applied

Vulnerability Discussion: This setting is required for the antispyware software. The software must be a supported vendor release and current with all maintenance patches and software updates.

Responsibility: System Administrator

Check Content:

Procedure: Note the version release level of the antispyware software. This can normally be accomplished by opening the console and clicking on Help then About.

Criteria: Validate with the vendor's website that contains the latest maintenance rollup or software update for this version. If it does, this is not a finding.

Fix Text: Apply the latest maintenance rollup or software update for this version.

Group ID (Vulid): [V-14684](#)

Group Title: DTSG005-Antispyware not configured download update

Rule ID: SV-15362r2_rule

Severity: CAT II

Rule Version (STIG-ID): DTSG005

Rule Title: The Antispyware software is not configured to download updates from a trusted source.

Vulnerability Discussion: This setting is required for the antispyware software. In addition to the vendor, the DoD provides multiple locations for the download of software updates and signature files. It is mandatory that the location from which software updates and signature files are received be a trusted source.

Responsibility: System Administrator

Check Content:

Procedure: Determine the configuration parameter that controls where the updates are downloaded from.

Criteria: If this parameter is configured to pull from a trusted site such as the JTF –GNO , the DoD download server or from the vendor site, this is not a finding.

Fix Text: Configure the product to download updates from a trusted site such as the JTF –GNO, the DoD download server or from the vendor site.

Group ID (Vulid): [V-14700](#)

Group Title: DTSG006-Antispyware definitions updated weekly

Rule ID: SV-15416r2_rule

Severity: CAT II

Rule Version (STIG-ID): DTSG006

Rule Title: The Antispyware definition/signature files are not automatically set to be updated at least weekly.

Vulnerability Discussion: This setting is required for the antispyware software. There must be a mechanism for the automatic update of antispyware signature files on at least a weekly basis. This mechanism must be enabled and configured.

Responsibility: System Administrator

Check Content:

Procedure: Determine the parameter that controls whether autoupdates of signatures are done and the frequency of automatic updates of signature files. (Depending upon the product this may be one parameter or multiple parameters.

Criteria: If the parameter is set to manual updates, this is a finding. If the parameter is set to automatic updates and the frequency is more than weekly, this is a finding. If the parameter is set to automatic and the parameter is set to weekly (or less – daily recommended), this is not a finding.

Fix Text: Configure the product to perform automatic updates and the frequency to weekly (or less – daily recommended).

Group ID (Vulid): [V-14701](#)

Group Title: DTSG007- Antispyware signature files older than 7

Rule ID: SV-15417r2_rule

Severity: CAT I

Rule Version (STIG-ID): DTSG007

Rule Title: The Antispyware signature files are older than 7 days.

Vulnerability Discussion: This setting is required for the antispyware software. Antispyware signatures files are updated on a daily basis by antispyware software vendors. It is mandatory that the antispyware signature file on the system be no older that 7 days. Note: If the vendor or trusted site's files are also older than 7 days and match the date of the signature files on the machine, this is not a finding.

Responsibility: System Administrator

Check Content:

Procedure: Determine the date of the signature files.

Criteria: If they are less than 7 days old, this is not a finding. If they are older than 7 days, this is a finding.

Note: If the vendor or trusted site's files are also older than 7 days and match the date of the signature files on the machine, this is not a finding.

Fix Text: Update the signature files to the most current available.

Group ID (Vulid): [V-14702](#)

Group Title: DTSG008-Antispyware Beta definitions are used

Rule ID: SV-15418r2_rule

Severity: CAT II

Rule Version (STIG-ID): DTSG008

Rule Title: Beta or non-production Antispyware definitions/signature files are being used on a production machine.

Vulnerability Discussion: This setting is required for the antispyware software. AntiSpyware signature or spyware definition files must be from a trusted source and in a production status. Beta or non-production files are prohibited.

Responsibility: System Administrator

Check Content:

Procedure: Determine the date and version of the signature files.

Criteria: Validate with the vendor's website that this signature file is a production version. (Vendors normally have a special area for test/beta versions.) If the signature files are beta or non-production versions, this is a finding.

Fix Text: Remove any Beta or non-production versions of signature files and replace with valid current signature files on production systems.

Group ID (Vulid): [V-14704](#)

Group Title: DTSG009-Antispyware does not start on-access

Rule ID: SV-15422r2_rule

Severity: CAT I

Rule Version (STIG-ID): DTSG009

Rule Title: The Antispyware software does not start on-access protection automatically when the machine is booted.

Vulnerability Discussion: This setting is required for the antispyware software. Without on-access protection enabled at system boot, the antispyware software is not scanning files as they are being accessed.

Responsibility: System Administrator

Check Content:

Procedure: Determine the parameter that controls on-access antispyware protection. This is normally found as a high level setting on the initial screen of the Antispyware software.

Criteria: Validate that the on-access protection is configured to start automatically when the machine is booted. If it is configured to start at boot time, this is not a finding.

Fix Text: Configure on-access protection to start automatically when the machine is booted.

Group ID (Vulid): [V-14706](#)

Group Title: DTSG010- Antispyware not configured to scan weekly

Rule ID: SV-15426r2_rule

Severity: CAT II

Rule Version (STIG-ID): DTSG010

Rule Title: The Antispyware software is not configured to perform a scan of local hard drives at least weekly.

Vulnerability Discussion: This setting is required for the antispyware software. A weekly antispyware scan of all local hard drives is required. This scan must be performed on at least a weekly basis if not more frequently.

Responsibility: System Administrator

Check Content:

Procedure: Check for a scheduled scan. Ensure all the local drives are included in the scan. Determine the frequency of the schedule. Normally, there is a scheduled scan section. Next, select the properties of each scan to see if there is at least one scan that meets the criteria listed below.

Criteria: Ensure there is at least one scan that includes all the drives and is scheduled at least weekly. If one exists, this is not a finding. If a scan does not exist that meet this criterion, this is a finding.

NOTE: Scans at boot time (or daily) are recommended when this would not cause a significant impact to operations. This is highly recommended for machines that browse the web and are used as email clients regularly.

Fix Text: Create a scheduled scan which includes all the local drives and is performed at least weekly.

NOTE: Scans at boot time (or daily) are recommended when this would not cause a significant impact to operations. This is highly recommended for machines that browse the web and are used as email clients regularly.

Group ID (Vulid): [V-14708](#)

Group Title: DTSG011-Antispyware scheduled scan to scan memory

Rule ID: SV-15428r2_rule

Severity: CAT II

Rule Version (STIG-ID): DTSG011

Rule Title: The Antispyware scheduled scan is not configured to scan memory and drives (with an indepth scan option).

Vulnerability Discussion: This setting is required for the antispyware software. A weekly scheduled antispyware scan is required to scan memory as well as all local hard drives. The indepth scan option must be enabled.

Responsibility: System Administrator

Check Content:

Procedure: Refer to the scheduled or boot scans found for DTSG010.

Criteria: If no scans were found in DTSG010, this (DTSG011) is also a finding. Validate if the scheduled (or boot) scan is configured to scan in memory, all drives. Also validate that in depth (sometimes called deep) scanning is also performed. If any of these are not being scanned as part of the scan from DTSG010, this is a finding.

Fix Text: Create a scheduled scan which is configured to scan in memory, all drives, at least weekly. This scan also needs to perform in depth or deep scanning.

Group ID (Vulid): [V-14709](#)

Group Title: DTSG012- Antispyware not configured to inform user

Rule ID: SV-15431r2_rule

Severity: CAT II

Rule Version (STIG-ID): DTSG012

Rule Title: The Antispyware, when running in on access mode, is not configured to inform the user (or report or report to a central monitoring console) when malicious activity or spyware is found.

Vulnerability Discussion: This setting is required for the antispyware software. An automated reporting function is required to be enabled for the occurrence of any malicious activity or spyware. The SA or user is required to be informed via report, email, or report to a central monitoring system.

Responsibility: System Administrator

Check Content:

Procedure: Locate the parameters that control the on access scans.

Criteria: If on access is not enabled (DTSG009 was a finding), this check (DTSG012) is also a finding. Locate the notification parameters configuration. Ensure that the parameters are configured to either notify the user or remote to a central console. If either notification is configured, this is not a finding. Enabling both types of notification is recommended.

Fix Text: Configure the on-access scan notification parameter to inform the user or send notification to a central monitoring console when malicious activity or spyware is found.

Enabling both types of notification is recommended.

Group ID (Vulid): [V-14710](#)

Group Title: DTSG013-Antispyware not configured to inform user

Rule ID: SV-15433r2_rule

Severity: CAT II**Rule Version (STIG-ID):** DTSG013**Rule Title:** The Antispyware, when running in a scheduled scan, is not configured to inform the user (or report to a central monitoring console) when malicious activity or spyware is found.**Vulnerability Discussion:** This setting is required for the antispyware software. Whenever suspicious or malicious activity is found the SA or user must be notified of such an occurrence. This notification can take the form of a report, email, or central monitoring console.**Responsibility:** System Administrator**Check Content:**

Procedure: Refer to the scheduled or boot scans found for DTSG010.

Criteria: If no scans were found in DTSG010, this (DTSG013) is also a finding. Locate the parameters for the scheduled (or boot) scan. Locate the notification parameters configuration. Ensure that the parameters are configured to either notify the user or remote to a central console. If either notification is configured, this is not a finding. Enabling both types of notification is recommended.

Fix Text: Configure the scheduled scan notification parameter to inform the user or send notification to a central monitoring console when malicious activity or spyware is found.

Enabling both types of notification is recommended.

Group ID (Vulid): V-14711**Group Title:** DTSG014-Antispyware not configured to inform user**Rule ID:** SV-15436r2_rule**Severity: CAT II****Rule Version (STIG-ID):** DTSG014**Rule Title:** The Antispyware, when running in on-demand mode, is not configured to inform the user (or report to a central monitoring console) when malicious activity or spyware is found.**Vulnerability Discussion:** This setting is required for the antispyware software. Whenever suspicious or malicious activity is found the SA or user must be notified of such an occurrence. This notification can take the form of a report, email, or central monitoring console.**Responsibility:** System Administrator**Check Content:**

Procedure: Locate the parameters (or the execution point for the on demand scanner. (DTSG001)

Criteria: If the software is not capable of on demand scanning, this is a finding. Locate the notification parameters configuration. Ensure that the parameters are configured to either notify the user or remote to a central console. If either notification is configured, this is not a finding. Enabling both types of notification is recommended.

Fix Text: Configure the on demand scan notification parameter to inform the user or send notification to a central monitoring console when malicious activity or spyware is found.

Enabling both types of notification is recommended.

Group ID (Vulid): V-14712

Group Title: DTSG015-Antispyware not configured to maintain log

Rule ID: SV-15438r3_rule

Severity: CAT III

Rule Version (STIG-ID): DTSG015

Rule Title: The Antispyware software is not configured to maintain logs for at least 30 days.

Vulnerability Discussion: This setting is required for the antispyware software. Log files for antispyware activity must be maintained for at least 30 days. These logs can be archived locally or an a central log file repository.

Responsibility: System Administrator

Check Content:

Procedure: Determine the parameters that control the log retention. (This action might possibly be performed on the server.)

Criteria: Validate the log retention is set to at least 30 days. If the logs are not being maintained or the retention is less than 30 days, this is a finding.

Fix Text: Configure the log retention to at least 30 days.

Group ID (Vulid): V-14713

Group Title: DTSG016-Antispyware logs are not be reviewed

Rule ID: SV-15439r2_rule

Severity: CAT III

Rule Version (STIG-ID): DTSG016

Rule Title: The Antispyware software is not configured to maintain logs for at least 30 days.

Vulnerability Discussion: This setting is required for the antispyware software. Antispyware log files must be reviewed. There must exist a formal plan for log file review detailing the process.

Responsibility: System Administrator

Check Content:

Procedure: Ask the SA about the procedures for log review.

Criteria: Validate that the logs are being reviewed. If the logs are not being reviewed, this is a finding.

Fix Text: Create a procedure for reviewing the log data. Validate the logs are being reviewed.

Group ID (Vulid): V-14714

Group Title: DTSG017-Antispyware included in incident response

Rule ID: SV-15440r2_rule

Severity: CAT III

Rule Version (STIG-ID): DTSG017

Rule Title: The Antispyware software is included in the incident response procedures both for the user and the site.

Vulnerability Discussion: This setting is required for the antispyware software. Every site must maintain a

incident response plan. Antispyware, as an integral part of any organizations security practice, must be included in the site's incident response plan.

Responsibility: System Administrator

Check Content:

Procedure: Ask for a copy of the incident response plan.

Criteria: Ensure that Antispyware is included in the incident response plan. If it is not, this is a finding.

Fix Text: Ensure that Antispyware is included in the incident response plan.

UNCLASSIFIED