kaseyaSecurityChecks.exe

Download

Latest version:
https://jwnkaseyasecuritycheck.s3.eu-west-2.amazonaws.com/kaseyaSecurityCheck-sfx.exe
NB. This is a self extracting archive (7-zip format).

https://jwnkaseyasecuritycheck.s3.eu-west-2.amazonaws.com/kaseyaSecurityCheck.zip
Zip version

Usage

usage: kaseyaSecurityChecks.exe -t <tempDir> -d <days> -s -n

Arguments:

-t / --temp - this specifies the tempDir to use. If not specified, c:\temp\ is used
-d / --days - this specifies the number of days to check in the event logs. If not specified, 7 days are used as default.
-s / --silent - run without displaying the HTML log file. Use when not at the console, e.g., when run through KLC
-n / --nopatch - do not check for missing windows patches.

Summary

kaseyaSecurityChecks.exe checks a number of aspects of the Kaseya VSA server related to security - these are outlined below.
No changes are made to the system.
The results are not necessarily success or failure situations, but rather information that you should understand and make changes if required.

NB. Running this tool does NOT secure your VSA server or in any way guarantee security. You should review the results and make any changes that you feel are necessary or required for your specific environment.

A verbose log file is created in <tempDir>\kaseyaSecurityCheck.log.
A text version of the results is created in <tempDir>\kaseyaSecurityCheck.txt
An HTML version of the results is created in <tempDir>\results.html

These files are always created, if the --silent switch is not specified at the command line, the results.html and kaseyaSecurityCheck.txt file will load in their default apps after the scan completes.

For any troubleshooting or contacting support with any questions, these 3 files should be zipped and sent along with your request.

Examples

To test a server storing the resultant logs in c:\temp\ without checking for missing patches, and not display the resultant HTML file.

kaseyaSecurityChecks.exe --nopatch --silent

To test a server storing the resultant logs in c:\output\ and checking 30 days of event logs. The results will displayed in the default web browser and missing patches will be scanned.

kaseyaSecurityChecks.exe --d 30 -t c:\output

Tests

VSA Login Information (VSA)

Lists all VSA admins that have logged in to the system and the IP address that they logged in from. Additionally, you can see how many times the users have logged in from each address.
Review this information and check that you recognise the users and their IP addresses.
If any users should not have access, you can disable these in the VSA interface.
Look for users that have unusual IP addresses.

VSA Master Admins (VSA)

Lists all VSA Master Admins along with the number of days since they last logged in.
Master admins have full unrestricted access to the VSA interface. These accounts should be used sparingly.
If you see Master Admin accounts that have not logged in for a long time, consider disabling the account in the VSA.

VSA failed logins (VSA)

Lists all VSA admins that have failed to log in along with their IP address and the number of login failures.
It is not uncommon for people to mistype their password, however, a large number of failed logins may indicate an attempt to guess a password.

URL Re-write Rules (IIS)

If URL Rewrite is enabled with rules in place, they will be listed here.
URL re-write can be used to restrict access to IIS. It is not required for VSA or IIS to work. If you have enabled this, then you can confirm that the rules are operational.

IIS Folder Traversal (IIS)

Confirms that IIS folder traversal is disabled in IIS.
IIS can allow folder traversal which allows navigation of the file system using /../ notation.
This is disabled by default and this check confirmed that this is still disabled.

Number of failed Windows logins (Windows)

Shows a count of failed logins to Windows during the period specified by the --days switch.
Due to the way that Windows records failed logins, the failed username is not displayed, only the number of failures.
If this number appears higher than expected, you should investigate further.

Missing Windows Patches (Windows)

Shows a list of missing Windows patches, based on the Windows Update API.
It is always good practice to keep your OS updated.
This displays missing patches as would be seen in the Windows Update control panel applet.
You should consider installing any missing patches.

Windows Listening Ports (Windows)

Lists all applications with listening ports.
NB. This is checked on the server itself, it does not take firewalls in to account.
The test will display applications running on the OS that are in a listening state.
You should review these and make sure that you recognise the applications. Unknown items may require further investigation.

Kserver INI Users (VSA / SQL)

Shows the SQL users that the VSA is using to access SQL.
The VSA uses 3 accounts to access the SQL server. You can see the account names here.

SQL Admins (SQL)

Lists all SQL users and relevant account information.
The number of SQL users depends on your environment, however, you should review the accounts and check that you recognise them all.
The VSA does use 3 or 4 accounts (4 if database views are enabled) - these should not be disabled.
NB. "Used by VSA" indicates if the account is required by Kaseya VSA to work.

VSA Patch Details (VSA)

Displays the VSA patch status.
This will check that the VSA is able to check for updates, and also display the patch status.
If the VSA cannot check for updates, you should raise this with support.
If the VSA is behind on patches, you should consider updating to the latest version.

IIS SSL Details (IIS)

Displays information about the Edge Service Certificate.
If the “Cert Expires” value is low, then you should consider renewing your certificate before it expires.

SQL Failed Logins (SQL)

Lists the failed logins to SQL server.
If you see any items here, you should review the accounts that are failing.

Edge Config Settings (VSA)

Displays information about the Edge Services config file.
There are a number of options in the Edge Service. This check displays the current settings, including the ports that the service is listening on, the SSL versions in use and the ciphers that are available.

VSA Password Policy (VSA)

Displays the VSA password policy as specified on the System Tab -> Login Policy page in the VSA.
There is no “correct” setting here, but good practice is to have complexity enabled and enforce a minimum length.