Scan Report

OS_INFO

System: Windows

Host Name: Harish

Release: 10

Version: 10.0.22631

Machine: AMD64

Processor: Intel64 Family 6 Model 186 Stepping 2, GenuineIntel

Python Version: 3.11.9

.Net Version

NO .NET Framework versions found.

Classic Audit Policies:

Error: Access is denied.

Advanced Audit Policies:

No essential advanced audit policies found or policies are not configured.

Autorun Programs

Registry Autorun Entries

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
SecurityHealth -> %windir%\system32\SecurityHealthSystray.exe

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
RtkAudUService -> "C:\Windows\System32\DriverStore\FileRepository\realtekservice.inf_amd64_a5b59

Scan Report

50537cd134e\RtkAudUService64.exe" -background

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] OneDrive -> "C:\Users\Harish\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] MicrosoftEdgeAutoLaunch_39E524273A6F5DF58A961A39D0DAD671 -> "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window --win-session-start

Scheduled Tasks

\ACCBackgroundApplication

\Adobe Acrobat Update Task

\App Explorer

\NitroSenseLauncher

\NVIDIA app SelfUpdate_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}

\NvProfileUpdaterDaily_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}

\NvProfileUpdaterOnLogon_{B2FE1952-0186-46C3-BAEC-A80AA35AC5B8}

\OneDrive Reporting Task-S-1-5-21-302543691-2197548985-1238483389-1003

\OneDrive Standalone Update Task-S-1-5-21-302543691-2197548985-1238483389-1003

\Software Update Application

\StorPSCTL

Scan Report

\CareCenter\CanvaAutoLaunchAvailabilityCheckAgent_Reg_HKCURun_S-1-5-21-302543691-2197548985-1238483389-1003

\Microsoft\Office\Office Automatic Updates 2.0

\Microsoft\Office\Office ClickToRun Service Monitor

\Microsoft\Office\Office Feature Updates

\Microsoft\Office\Office Feature Updates Logon

\Microsoft\Office\Office Performance Monitor

\Microsoft\Windows\Active Directory Rights Management Services Client\AD RMS Rights Policy Template Management (Manual)

\Microsoft\Windows\AppID\PolicyConverter

\Microsoft\Windows\AppID\VerifiedPublisherCertStoreCheck

\Microsoft\Windows\Application Experience\MareBackup

\Microsoft\Windows\Application Experience\Microsoft Compatibility Appraiser

\Microsoft\Windows\Application Experience\PcaPatchDbTask

\Microsoft\Windows\Application Experience\PcaWallpaperAppDetect

\Microsoft\Windows\Application Experience\SdbinstMergeDbTask

\Microsoft\Windows\Application Experience\StartupAppTask

\Microsoft\Windows\ApplicationData\appuriverifierdaily

\Microsoft\Windows\ApplicationData\appuriverifierinstall

\Microsoft\Windows\ApplicationData\CleanupTemporaryState

\Microsoft\Windows\ApplicationData\DsSvcCleanup

\Microsoft\Windows\AppListBackup\Backup

\Microsoft\Windows\AppListBackup\BackupNonMaintenance

\Microsoft\Windows\Autochk\Proxy

Scan Report

\Microsoft\Windows\BitLocker\BitLocker Encrypt All Drives

\Microsoft\Windows\BitLocker\BitLocker MDM policy Refresh

\Microsoft\Windows\Bluetooth\UninstallDeviceTask

\Microsoft\Windows\BrokerInfrastructure\BgTaskRegistrationMaintenanceTask

\Microsoft\Windows\capabilityaccessmanager\maintenancetasks

\Microsoft\Windows\CertificateServicesClient\UserTask

\Microsoft\Windows\CertificateServicesClient\UserTask-Roam

\Microsoft\Windows\Chkdsk\ProactiveScan

\Microsoft\Windows\CloudRestore\Backup

\Microsoft\Windows\CloudRestore\Restore

\Microsoft\Windows\ConsentUX\UnifiedConsent\UnifiedConsentSyncTask

\Microsoft\Windows\Customer Experience Improvement Program\Consolidator

\Microsoft\Windows\Data Integrity Scan\Data Integrity Check And Scan

\Microsoft\Windows\Data Integrity Scan\Data Integrity Scan

\Microsoft\Windows\Defrag\ScheduledDefrag

\Microsoft\Windows\Device Information\Device

\Microsoft\Windows\Device Information\Device User

\Microsoft\Windows\Diagnosis\RecommendedTroubleshootingScanner

\Microsoft\Windows\DiskCleanup\SilentCleanup

\Microsoft\Windows\DiskFootprint\Diagnostics

\Microsoft\Windows\DiskFootprint\StorageSense

\Microsoft\Windows\DUSM\dusmtask

\Microsoft\Windows\EDP\EDP App Launch Task

\Microsoft\Windows\EDP\EDP Auth Task

Scan Report

\Microsoft\Windows\EDP\EDP Inaccessible Credentials Task

\Microsoft\Windows\EDP\StorageCardEncryption Task

\Microsoft\Windows\ExploitGuard\ExploitGuard MDM policy Refresh

\Microsoft\Windows\Feedback\Siuf\DmClient

\Microsoft\Windows\Feedback\Siuf\DmClientOnScenarioDownload

\Microsoft\Windows\FileHistory\File History (maintenance mode)

\Microsoft\Windows\Flighting\FeatureConfig\ReconcileFeatures

\Microsoft\Windows\Flighting\FeatureConfig\UsageDataFlushing

\Microsoft\Windows\Flighting\FeatureConfig\UsageDataReporting

\Microsoft\Windows\Flighting\OneSettings\RefreshCache

\Microsoft\Windows\Input\InputSettingsRestoreDataAvailable

\Microsoft\Windows\Input\LocalUserSyncDataAvailable

\Microsoft\Windows\Input\MouseSyncDataAvailable

\Microsoft\Windows\Input\PenSyncDataAvailable

\Microsoft\Windows\Input\syncpensettings

\Microsoft\Windows\Input\TouchpadSyncDataAvailable

\Microsoft\Windows\InstallService\RestoreDevice

\Microsoft\Windows\InstallService\ScanForUpdates

\Microsoft\Windows\InstallService\ScanForUpdatesAsUser

\Microsoft\Windows\International\Synchronize Language Settings

\Microsoft\Windows\Kernel\La57Cleanup

\Microsoft\Windows\LanguageComponentsInstaller\Installation

\Microsoft\Windows\LanguageComponentsInstaller\ReconcileLanguageResources

\Microsoft\Windows\Location\Notifications

\Microsoft\Windows\Location\WindowsActionDialog

\Microsoft\Windows\Maintenance\WinSAT

\Microsoft\Windows\Management\Provisioning\Logon

\Microsoft\Windows\MUI\LPRemove

\Microsoft\Windows\Multimedia\SystemSoundsService

\Microsoft\Windows\NetTrace\GatherNetworkInfo

\Microsoft\Windows\PI\SecureBootEncodeUEFI

\Microsoft\Windows\Plug and Play\Sysprep Generalize Drivers

\Microsoft\Windows\Power Efficiency Diagnostics\AnalyzeSystem

\Microsoft\Windows\Printing\EduPrintProv

\Microsoft\Windows\Printing\PrinterCleanupTask

\Microsoft\Windows\Security\Pwdless\IntelligentPwdlessTask

\Microsoft\Windows\Servicing\StartComponentCleanup

\Microsoft\Windows\Shell\FamilySafetyMonitor

\Microsoft\Windows\Shell\FamilySafetyRefreshTask

\Microsoft\Windows\Shell\IndexerAutomaticMaintenance

\Microsoft\Windows\Shell\ThemesSyncedImageDownload

\Microsoft\Windows\SpacePort\SpaceAgentTask

\Microsoft\Windows\SpacePort\SpaceManagerTask

\Microsoft\Windows\StateRepository\MaintenanceTasks

\Microsoft\Windows\Storage Tiers Management\Storage Tiers Management Initialization

\Microsoft\Windows\Sysmain\ResPriStaticDbSync

\Microsoft\Windows\Sysmain\WsSwapAssessmentTask

\Microsoft\Windows\SystemRestore\SR

\Microsoft\Windows\Time Synchronization\ForceSynchronizeTime

\Microsoft\Windows\Time Synchronization\SynchronizeTime

\Microsoft\Windows\Time Zone\SynchronizeTimeZone

\Microsoft\Windows\UPnP\UPnPHostConfig

\Microsoft\Windows\Windows Defender\Windows Defender Cache Maintenance

\Microsoft\Windows\Windows Defender\Windows Defender Cleanup

\Microsoft\Windows\Windows Defender\Windows Defender Scheduled Scan

\Microsoft\Windows\Windows Defender\Windows Defender Verification

\Microsoft\Windows\Windows Error Reporting\QueueReporting

\Microsoft\Windows\Windows Media Sharing\UpdateLibrary

\Microsoft\Windows\WindowsColorSystem\Calibration Loader

\Microsoft\Windows\WindowsUpdate\Scheduled Start

\Microsoft\Windows\Wininet\CacheTask

\Microsoft\Windows\WlanSvc\CDSSync

\Microsoft\Windows\WlanSvc\MoProfileManagement

\Microsoft\Windows\Work Folders\Work Folders Logon Synchronization

\Microsoft\Windows\Work Folders\Work Folders Maintenance Work

\Microsoft\Windows\WwanSvc\OobeDiscovery

\Microsoft\XblGameSave\XblGameSaveTask

\Oem\AcerJumpstartTask

Startup Folder Entries

Scan Report

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini

C:\Users\Harish\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini

Essential Windows Defender Settings

RealTimeProtectionEnabled: True

AntivirusEnabled: True

SignatureUpToDate: None

LastQuickScanTime: None

ScanScheduleDay: 0

ScanScheduleTime: {'Ticks': 72000000000, 'Days': 0, 'Hours': 2, 'Milliseconds': 0, 'Minutes': 0, 'Seconds': 0, 'TotalDays': 0.08333333333333333, 'TotalHours': 2, 'TotalMilliseconds': 7200000, 'TotalMinutes': 120, 'TotalSeconds': 7200}

Firewall Issues

No critical firewall vulnerabilities found.

Hotfixes

Caption CSName Description FixComments HotFixID InstallDate InstalledBy InstalledOn Name ServicePackInEffect Status

http://support.microsoft.com/?kbid=5045935 HARISH Update KB5045935 NT AUTHORITY\SYSTEM 11/15/2024

https://support.microsoft.com/help/5027397 HARISH Update KB5027397 NT AUTHORITY\SYSTEM 9/14/2024

Scan Report

https://support.microsoft.com/help/5046633 HARISH Security Update KB5046633 NT AUTHORITY\SYSTEM 11/15/2024

HARISH Security Update KB5046247 NT AUTHORITY\SYSTEM 10/19/2024

HARISH Update KB5044620 NT AUTHORITY\SYSTEM 11/15/2024

Local User Accounts

Name: Administrator, Enabled: False, LastLogon: /Date(1705663208193)/

Name: DefaultAccount, Enabled: False, LastLogon: None

Name: Guest, Enabled: False, LastLogon: None

Name: Harish, Enabled: True, LastLogon: /Date(1725120957557)/

Name: WDAGUtilityAccount, Enabled: False, LastLogon: None

Pending Updates

No pending updates found.