# Scan Report

## OS_INFO

System: Windows

Host Name: MSI

Release: 11

Version: 10.0.22631

Machine: AMD64

Processor: Intel64 Family 6 Model 140 Stepping 2, GenuineIntel

Python Version: 3.13.1

## .Net Version

NO .NET Framework versions found.

## Classic Audit Policies:

File Path: %SystemRoot%\System32\winevt\Logs\Security.evtx

Max Size: 20 MB

Retention Policy: 0

Restrict Guest Access: 1

## 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

# Scan Report

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run] RtkAudUService -> "C:\Windows\System32\DriverStore\FileRepository\realtekservice.inf_amd64_2f3cb0b10cd40ee4\RtkAudUService64.exe" -background

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

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] MicrosoftEdgeAutoLaunch_1F8F8450CAC46604C2DCB438C17C0920 -> "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window --win-session-start

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] org.openvpn.client -> C:\Program Files\OpenVPN Connect\OpenVPNConnect.exe --opened-at-login --minimize

Scheduled Tasks

\MicrosoftEdgeUpdateTaskMachineCore

\MicrosoftEdgeUpdateTaskMachineUA

\npcapwatchdog

\OneDC_Updater

\OneDrive Reporting Task-S-1-5-21-3038702317-1907410546-2142576592-1001

\OneDrive Standalone Update Task-S-1-5-21-3038702317-1907410546-2142576592-1001

# Scan Report

\OneDrive Standalone Update Task-S-1-5-21-3038702317-1907410546-2142576592-500

\Microsoft\Office\Office 15 Subscription Heartbeat

\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\Office\OfficeTelemetryAgentFallBack

\Microsoft\Office\OfficeTelemetryAgentLogOn

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

\Microsoft\Windows\AppID\EDP Policy Manager

\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

# Scan Report

\Microsoft\Windows\AppListBackup\BackupNonMaintenance

\Microsoft\Windows\Autochk\Proxy

\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\AikCertEnrollTask

\Microsoft\Windows\CertificateServicesClient\CryptoPolicyTask

\Microsoft\Windows\CertificateServicesClient\KeyPreGenTask

\Microsoft\Windows\CertificateServicesClient\SystemTask

\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\Device Information\Device

\Microsoft\Windows\Device Information\Device User

\Microsoft\Windows\Diagnosis\RecommendedTroubleshootingScanner

\Microsoft\Windows\DiskCleanup\SilentCleanup

# Scan Report

\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

\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

# Scan Report

\Microsoft\Windows\InstallService\SmartRetry

\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\Mcbuilder

\Microsoft\Windows\Multimedia\SystemSoundsService

\Microsoft\Windows\NetTrace\GatherNetworkInfo

\Microsoft\Windows\PI\Secure-Boot-Update

\Microsoft\Windows\PI\SecureBootEncodeUEFI

\Microsoft\Windows\PI\Sqm-Tasks

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

\Microsoft\Windows\Power Efficiency Diagnostics\AnalyzeSystem

\Microsoft\Windows\Printing\EduPrintProv

\Microsoft\Windows\Printing\PrinterCleanupTask

\Microsoft\Windows\PushToInstall\LoginCheck

\Microsoft\Windows\PushToInstall\Registration

\Microsoft\Windows\Ras\MobilityManager

\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\Shell\UpdateUserPictureTask

\Microsoft\Windows\SpacePort\SpaceAgentTask

\Microsoft\Windows\SpacePort\SpaceManagerTask

\Microsoft\Windows\Speech\SpeechModelDownloadTask

\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\TPM\Tpm-HASCertRetr

\Microsoft\Windows\TPM\Tpm-Maintenance

\Microsoft\Windows\UpdateOrchestrator\Report policies

\Microsoft\Windows\UpdateOrchestrator\Schedule Scan

\Microsoft\Windows\UpdateOrchestrator\Schedule Scan Static Task

\Microsoft\Windows\UpdateOrchestrator\Schedule Work

\Microsoft\Windows\UpdateOrchestrator\Start Oobe Expedite Work

\Microsoft\Windows\UpdateOrchestrator\StartOobeAppsScanAfterUpdate

\Microsoft\Windows\UpdateOrchestrator\StartOobeAppsScan_LicenseAccepted

\Microsoft\Windows\UpdateOrchestrator\USO_UxBroker

\Microsoft\Windows\UpdateOrchestrator\UUS Failover Task

\Microsoft\Windows\UPnP\UPnPHostConfig

\Microsoft\Windows\WaaSMedic\PerformRemediation

\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\Refresh Group Policy Cache

\Microsoft\Windows\WindowsUpdate\Scheduled Start

\Microsoft\Windows\Wininet\CacheTask

\Microsoft\Windows\WlanSvc\CDSSync

\Microsoft\Windows\WlanSvc\MoProfileManagement

\Microsoft\Windows\WOF\WIM-Hash-Management

\Microsoft\Windows\WOF\WIM-Hash-Validation

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

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

\Microsoft\Windows\WwanSvc\OobeDiscovery

\Microsoft\XblGameSave\XblGameSaveTask

\Norton 360\Norton 360 Autofix

\Norton 360\Norton 360 Error Analyzer

\Norton 360\Norton 360 Error Processor

\Remediation\AntimalwareMigrationTask

Startup Folder Entries

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

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

C:\Users\steph\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Send to OneNote.lnk

## 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

# Scan Report

Caption CSName Description FixComments HotFixID InstallDate InstalledBy InstalledOn Name ServicePackInEffect Status

http://support.microsoft.com/?kbid=5045935 MSI Update KB5045935 NT AUTHORITY\SYSTEM 12/13/2024

https://support.microsoft.com/help/5027397 MSI Update KB5027397 NT AUTHORITY\SYSTEM 4/5/2024

https://support.microsoft.com/help/5031274 MSI Update KB5031274 NT AUTHORITY\SYSTEM 1/18/2024

https://support.microsoft.com/help/5033055 MSI Update KB5033055 NT AUTHORITY\SYSTEM 1/18/2024

https://support.microsoft.com/help/5046633 MSI Security Update KB5046633 NT AUTHORITY\SYSTEM 12/13/2024

MSI Update KB5044620 NT AUTHORITY\SYSTEM 11/22/2024

# Scan Report

## Local User Accounts

Name: Administrator, Enabled: False, LastLogon: /Date(1693068033630)/

Name: DefaultAccount, Enabled: False, LastLogon: None

Name: Guest, Enabled: False, LastLogon: None

Name: steph, Enabled: True, LastLogon: None

Name: WDAGUtilityAccount, Enabled: False, LastLogon: None

## Pending Updates

No pending updates found.