System Hardening Worksheet

Hardware and Software List

Device/Host Name/Software	Version	Manufacturer	Model Number	Purpose
MACOS UTM virtual machine	QEMU 7.2 ARM Virtual machine	UTM	UTM Wndows 11	Host a virtual machine
MICROSOFT EDGE	119.0.2151.72	Microsoft	[N/A]	[Report viewing, and web browsing]
Section 2.0 Vulnerabilities From your scans, select FIFTEEN (15) Vulnerabilities that you are investigating. I advise starting with CAT-I (High/Criticals) if you'd interested in securing your system. And fill in the fields for Vulnerability Investigation		*Total Number of Vulnerabilities in your SCC/SCAP scan of your OS*	Windows operating system vulnerabilities: 123|Microsoft Edge Vulnerabilities: 49	

Vulnerability Investigation

Testing Source (which STIG)	Vulnerability ID (This should be V-#### from STIG Viewer)	RESULT (Open/Not a Finding/ Not Applicable)	CIA Triad Impact	NIST 800-53 Security Control Affected (short description. If Vuln has multiple, pick one). Refer to https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf for reference, after looking at the security control info in Stig Viewer.
Windows 11 STIG, v1 r3_Benchmark	[V-253505]	[Open]	This vulnerability gives an attacker the ability to overwrite and alter files/folders on a computer. The impact would be on integrity of the CIA triad as accuracy and reliability is affected.	This control is related to least privilege access by restricting privileged accounts on a system and reduces the risk of unauthorized access. This control also allows for diversity in personnel, ensuring critical tasks are distributed, which eliminates single point of failure. (NIST 800 53 AC-6(10))
Windows 11 STIG, v1 r3_Benchmark	V-253495	[Open]	Logon denial account rights define which accounts are prevented from logging in through remote desktop services. This is succeptible to credential theft attacks. The impact would be on availability of the CIA triad as not all accounts are given remote desktop services.	This control is related to least privilege access by restricting privileged accounts on a system and reduces the risk of unauthorized access. This control also allows for diversity in personnel, ensuring critical tasks are distributed, which eliminates single point of failure. (NIST 800 53 AC-3)
Windows 11 STIG, v1 r3_Benchmark	V-253494	[Open]	Logon denial account rights define which accounts are prevented from logging in through local devices. This is succeptible to privilege escalation from credential theft attacks. The impact would be on availability of the CIA triad as not all accounts are given remote desktop services.	This control is related to least privilege access by restricting privileged accounts on a system and reduces the risk of unauthorized access. This control also allows for diversity in personnel, ensuring critical tasks are distributed, which eliminates single point of failure. (NIST 800 53 AC-3)
Windows 11 STIG, v1 r3_Benchmark	V-253491	[Open]	This is related to denying access to a system from logging in on a network. The impact would be on availability of the CIA triad as only certain systems on the network are granted access to information.	This control is related to least privilege access by restricting privileged accounts on a system and reduces the risk of unauthorized access. This control also allows for diversity in personnel, ensuring critical tasks are distributed, which eliminates single point of failure.(NIST 800 53 AC-3
Windows 11 STIG, v1 r3_Benchmark	V-253483	[Open]	This is succeptible to bypassing secrurity restrictions and having unzauthorized access to files. The impact would be on confidentiality of the CIA triad as unauthorized access to files is compromised.	This control is related to least privilege access, emphasizing the importance of not allowing users to have unnecessary access to certain privileges and only to the controls necessary for certain users to get achieve their job duties. (NIST 800 53 AC-6(10))
Windows 11 STIG, v1 r3_Benchmark	V-253462	Open	This is an authentication protocol which is not secure for users logging into domain accounts. This affects availbility as the authentication protocol purpose is to maintain compatibility with older windows operating systems.	This control is related to configuration management for systems of an organization. This also ensures each system is configured to an organizations operational baseline. (NIST 800 53 CM-6B)
Windows 11 STIG, v1 r3_Benchmark	V-253454	Open	This vulnerability allows an attacker to remain anonymous while being able to list list account names and shared resources. This impacts confidentiality of the CIA triad as an attacker could map out potential points to attack in a system.	This control is related to information in shared resources. This also addresses the need to restrict and monitor access to shared resources, preventing unauthorized users from accessing sensitive information. (NIST 800 53 SC-4)
Windows 11 STIG, v1 r3_Benchmark	V-253416	Open	This vulnerability affects confidentiality as clients have a basic authentication using plain text passwords that would lead to systems being compromised.	This control employs strong authentication for system maintenance or diagnostic. (NIST 800 53 MA-4)
Windows 11 STIG, v1 r3_Benchmark	V-253411	Open	This vulnerability affects confidentiality as standard user accounts have access to elevated privileges and sensitive information.	This control is related to configuration management; establishing and enforcing security configurations. This control specifically prohibits installation of software without explicit privilege status. (NIST 800 53 CM-11(2))

Windows 11 STIG, v1 r3_Benchmark	V-253388	Open	This vulnerability affects confidentiality as having drivers on autoplay may result in malicious code being executed to compromise an organization's system.	This control dictates which programs organizations are allowed to run based on system configurations and baselines set by system administrators. (NIST 800 53 CM-7(2))
Microsoft Edge STIG v1r7	V-235759	Open	This sets the minimum supported secure shell socket and transport layer security. Integrity of the CIA triad is affected as the system only allows of the an approved version of secure shell socket and transport layer security for communication between a web server and user system.	This controls implements cryptographic mechanisms to protect confidentiality of web server sessions. (NIST 800 53 AC-17(2))
Microsoft Edge STIG v1r8	V-246736	Open	This vulnerability impacts confidentiality of the CIA triad with the possibility of exposing data in transit	This control limits users of an organization to only have the necessary actions needed to finish a job rather than having access to uneccessary configurations, implementing least functions. (NIST 800 53 MC-7)
Microsoft Edge STIG v1r9	V-235774	Open	This vulnerability impact availability of the CIA triad as communcation with the DNS servers are affected depending on system configurations.	This control implements replay resistant controls blocking network access to accounts that do not have privilege or administrative privileges. (NIST 800 52 IA-2(9))
Microsoft Edge STIG v1r10	V-235767	Open	This vulnerability impacts confidentiality of the CIA triad, as leaving this option enabled websites are able to access a user's payment information.	This control limits access to components of a systems inventory in information technology of an organization. In this case, this control is specific to payment methods saved to a system. (NIST 800 53 CM-8))
Microsoft Edge STIG v1r11	V-235756	Open	This vulnerability impacts confidentiality of the CIA triad, as allowing broswers to save passwords may potentially expose sensitive information.	This control has an expiry on cahced authenticators over a certain period of time (NIST 800 53 IA-5(13)