Compliance Report

Execution Date: 2024-06-14
Scoring: 7.69%

TITLE	NUMBER	PROFILE	DESCRIPTION	PASS
Ensure mounting of cramfs filesystems is disabled	1.1.1.1	Level 1 - Server, Level 1 - Workstation	The cramfs filesystem type is a compressed read - only Linux filesystem embedded in small footprint systems.A cramfs image can be used without having to first decompress it. This can be used to mount the image.	No
Ensure mounting of squashfs filesystems is disabled	1.1.1.2	Level 2 - Server, Level 2 - Workstation	The squashfs filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems. A squashfs image can be used without having to first decompress it. Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it. Impact: As Snap packages utilizes squashfs as a compressed filesystem, disabling squashfs will cause Snap packages to fail. Snap application packages of software are self-contained and work across a range of Linux distributions. This is unlike traditional Linux package management approaches, like APT or RPM, which require specifically adapted packages per Linux distribution on an application update and delay therefore application deployment from developers to their software's end-user. Snaps themselves have no dependency on any external store ("App store"), can be obtained from any source and can be therefore used for upstream software deployment.	No
Ensure mounting of udf filesystems is disabled	1.1.1.3	Level 2 - Server, Level 2 - Workstation	The udf filesystem type is the universal disk format used to implement ISO/IEC 13346 and ECMA-167 specifications. This is an open vendor filesystem type for data storage on a broad range of media. This filesystem type is necessary to support writing DVDs and newer optical disc formats. Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it. Impact: Microsoft Azure requires the usage of udf. udf should not be disabled on systems run on Microsoft Azure.	No

Ensure /tmp is a separate partition	1.1.2.1	Level 1 - Server, Level 1 - Workstation	The /tmp directory is a world-writable directory used for temporary storage by all users and some applications. Making /tmp its own file system allows an administrator to set additional mount options such as the noexec option on the mount, making /tmp useless for an attacker to install executable code. It would also prevent an attacker from establishing a hard link to a system setuid program and wait for it to be updated. Once the program was updated, the hard link would be broken and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw. This can be accomplished by either mounting tmpfs to /tmp, or creating a separate partition for /tmp.	No
Ensure nodev option set on /tmp partition	1.1.2.2	Level 1 - Server, Level 1 - Workstation	The nodev mount option specifies that the filesystem cannot contain special devices. Since the /tmp filesystem is not intended to support devices, set this option to ensure that users cannot create a block or character special devices in /tmp.	No

Ensure separate partition exists for /var/tmp	1.1.4.1	Level 2 - Server, Level 2 - Workstation	The /var/tmp directory is a world-writable directory used for temporary storage by all users and some applications. Temporary file residing in /var/tmp is to be preserved between reboots. The reasoning for mounting /var/tmp on a separate partition is as follow. Protection from resource exhaustion The default installation only creates a single / partition. Since the /var directory may contain world-writable files and directories, there is a risk of resource exhaustion. It will essentially have the whole disk available to fill up and impact the system as a whole. In addition, other operations on the system could fill up the disk unrelated to /var and cause unintended behavior across the system as the disk is full. See man auditd.conf for details. Fine grained control over the mount Configuring /var as its own file system allows an administrator to set additional mount options such as noexec/nosuid/nodev. These options limit an attacker's ability to create exploits on the system. Other options allow for specific behavior. See man mount for exact details regarding filesystem-independent and filesystem-specific options. Protection from exploitation An example of exploiting /var may be an attacker establishing a hard-link to a system setuid program and wait for it to be updated. Once the program was updated, the hard-link would be broken and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw. Impact: Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.	No

Ensure separate partition exists for /var/log	1.1.5.1	Level 2 - Server, Level 2 - Workstation	The /var/log directory is used by system services to store log data. The reasoning for mounting /var/log on a separate partition is as follow. Protection from resource exhaustion The default installation only creates a single / partition. Since the /var directory may contain world-writable files and directories, there is a risk of resource exhaustion. It will essentially have the whole disk available to fill up and impact the system as a whole. In addition, other operations on the system could fill up the disk unrelated to /var and cause unintended behavior across the system as the disk is full. See man auditd.conf for details. Fine grained control over the mount Configuring /var as its own file system allows an administrator to set additional mount options such as noexec/nosuid/nodev. These options limit an attacker's ability to create exploits on the system. Other options allow for specific behavior. See man mount for exact details regarding filesystem-independent and filesystem-specific options. Protection from exploitation An example of exploiting /var may be an attacker establishing a hard-link to a system setuid program and wait for it to be updated. Once the program was updated, the hard-link would be broken and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw. Impact: Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.	No
Ensure AIDE is installed	1.3.1	Level 1 - Server, Level 1 - Workstation	Advanced Intrusion Detection Environment (AIDE) is an intrusion detection tool that uses predefined rules to check the integrity of files and directories in the Linux operating system. AIDE has its own database to check the integrity of files and directories. AIDE takes a snapshot of files and directories including modification times, permissions, and file hashes which can then be used to compare against the current state of the filesystem to detect modifications to the system. By monitoring the filesystem state, compromised files can be detected to prevent or limit the exposure of accidental or malicious misconfigurations or modified binaries.	No

Ensure time synchronization is in use	2.1.1	Level 1 - Server, Level 1 - Workstation	System time should be synchronized between all systems in an environment. This is typically done by establishing an authoritative time server or set of servers and having all systems synchronize their clocks to them. Note: If another method for time synchronization is being used, this section may be skipped. Time synchronization is important to support time sensitive security mechanisms like Kerberos and also ensures log files have consistent time records across the enterprise, which aids in forensic investigations.	No
Verify if IPv6 is enabled on the system	3.1.1	Level 1 - Server, Level 1 - Workstation	Internet Protocol Version 6 (IPv6) is the most recent version of Internet Protocol (IP). It's designed to supply IP addressing and additional security to support the predicted growth of connected devices. It is recommended that either IPv6 settings are configured OR IPv6 be disabled to reduce the attack surface of the system. IETF RFC 4038 recommends that applications are built with an assumption of dual stack. If IPv6 is disabled through sysctl config, SSH X11forwarding may no longer function as expected. We recommend that SSH X11forwarding be disabled, but if required, the following will allow for SSH X11forwarding with IPv6 disabled through sysctl config: Add the following line the /etc/ssh/sshd_config file: AddressFamily inet Run the following command to re-start the openSSH server: # systemctl restart sshd	No
Ensure auditd is installed	4.1.1.1	Level 2 - Server, Level 2 - Workstation	auditd is the userspace component to the Linux Auditing System. It's responsible for writing audit records to the disk. The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.	No
Ensure cron daemon is enabled	5.1.1	Level 1 - Server, Level 1 - Workstation	The cron daemon is used to execute batch jobs on the system. While there may not be user jobs that need to be run on the system, the system does have maintenance jobs that may include security monitoring that have to run, and cron is used to execute them.	No
Ensure sticky bit is set on all world-writable directories	6.1.2	Level 1 - Server, Level 1 - Workstation	Setting the sticky bit on world writable directories prevents users from deleting or renaming files in that directory that are not owned by them. This feature prevents the ability to delete or rename files in world writable directories (such as /tmp) that are owned by another user.	Yes