OpenSCAP Triage Report

Target: 192.168.1.86 | Generated: 2026-02-12 02:29:59

Summary

Total Findings Triaged	19
Safe to Remediate	2
Requires Human Review	9
Too Dangerous / Blocked	8

Safe to Remediate (2)

ID	Risk	Reason	Impact
openscap_016	LOW	Sysctl persistence is unlikely to lock out access, and the change is low-risk.	—
openscap_018	LOW	The finding is related to the chronyd server directive, which is a configuration setting for the chrony time synchronization service. This is a low-risk change that is unlikely to cause issues with th	—

Requires Human Review (9)

ID	Risk	Reason	Impact
openscap_004	MEDIUM	SSH configuration changes may have unintended consequences on authentication and access	authentication/authorization affected; authn; access control
openscap_005	MEDIUM	SSH configuration changes may have unintended consequences on authentication and access	authentication/authorization affected; SSH configuration changes; potential access disruption
openscap_006	MEDIUM	The finding is related to the installed OS being vendor-supported, which may involve complex configuration or compatibility issues, requiring human review to ensure correct remediation.	OS configuration; vendor support
openscap_012	MEDIUM	The finding is related to authorized local users, which touches authentication and authorization.	authentication/authorization affected; authn; authz
openscap_013	MEDIUM	Changing the GRUB2 admin username may have unintended consequences on system authentication and authorization.	authentication/authorization affected; authn; authz
openscap_014	MEDIUM	Authentication/authorization hardening can lock out SSH/automation. Requires review and staged rollout.	authentication/authorization affected; networking affected; potential lockout; access control changes
openscap_015	MEDIUM	Name resolution configuration affects networking, which may have unintended consequences if not reviewed by a human.	networking affected; networking changes; potential connectivity issues

ID	Risk	Reason	Impact
openscap_017	MEDIUM	The finding involves SELinux context elevation for sudo, which is related to authentication and authorization.	authentication/authorization affected; authn; authz
openscap_019	MEDIUM	SSSD configuration changes may impact authentication and authorization	authentication/authorization affected; authn; authz

Too Dangerous to Remediate (8)

ID	Risk	Reason	Impact
openscap_001	CRITICAL	Enabling the dracut FIPS module may have unintended consequences on the system's boot process and partitioning.	reboot required; filesystems affected; FIPS changes; bootloader modifications
openscap_002	CRITICAL	FIPS mode changes can have significant impact on system functionality and compatibility	reboot required; system instability; compatibility issues
openscap_003	CRITICAL	FIPS changes can have significant impact on system security and functionality	reboot required; FIPS mode; system security; functionality impact
openscap_007	CRITICAL	Filesystem/partition/mount-option changes can break boot or services and should not be auto-remediated.	reboot required; filesystems affected; filesystems/partitioning; service disruption risk
openscap_008	CRITICAL	Filesystem/partition/mount-option changes can break boot or services and should not be auto-remediated.	reboot required; filesystems affected; filesystems/partitioning; service disruption risk
openscap_009	CRITICAL	Filesystem/partition/mount-option changes can break boot or services and should not be auto-remediated.	reboot required; filesystems affected; filesystems/partitioning; service disruption risk
openscap_010	CRITICAL	Filesystem/partition/mount-option changes can break boot or services and should not be auto-remediated.	reboot required; filesystems affected; filesystems/partitioning; service disruption risk
openscap_011	CRITICAL	Filesystem/partition/mount-option changes can break boot or services and should not be auto-remediated.	reboot required; filesystems affected; filesystems/partitioning; service disruption risk