OpenSCAP Triage Report

Target: 10.244.72.95 | Generated: 2026-02-12 12:48:42

Scan Statistics

Total Rules Scanned	1523
Rules Passed	1502
Rules Failed / Errors	21

Triage Summary

Total Findings Triaged	21
Safe to Remediate	2
Requires Human Review	11
Too Dangerous / Blocked	8

Safe to Remediate (2)

ID	Risk	Reason	Impact
openscap_015	LOW	Sysctl persistence is unlikely to lock out access and is a low-risk change.	—
openscap_017	LOW	Postfix configuration change to prevent unrestricted relay is a low-risk remediation.	networking affected

Requires Human Review (11)

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 system access	authentication/authorization affected; SSH access disruption; unintended configuration changes
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

ID	Risk	Reason	Impact
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_016	MEDIUM	The finding involves SELinux context elevation for sudo, which is related to authentication and authorization.	authentication/authorization affected; authn; authz
openscap_018	MEDIUM	The finding is related to the chronyd server directive, which may impact time synchronization and potentially affect system behavior. While the severity is moderate, it's unclear what specific changes	system behavior; time synchronization
openscap_019	MEDIUM	Disabling root login via SSH is a security best practice, but may have unintended consequences if not properly configured.	authentication/authorization affected; potential disruption to SSH access
openscap_020	MEDIUM	SSSD configuration changes may impact authentication and authorization	authentication/authorization affected; authn; authz
openscap_021	MEDIUM	The finding is related to configuring USBGuard audit backend, which may have implications on system security and access control.	authentication/authorization affected; potential impact on system security; possible changes to audit logging

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 security	reboot required; filesystems affected; partitioning; filesystem; bootloader; FIPS
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