Speakerbus

Title	SA-020 External Penetration Test (September 2024) Additional Remediations Report
Security Advisory Number	Various
Affected Product(s)	QORUS Infrastructure
TAC Reference	N/A
Audience	Operations, Clients, Partners
Date	03 April 2025
Supersede	SA-019
Severity	Medium/Low

Background:

In September 2024, our penetration testing assessment identified several high-severity and medium Common Vulnerabilities and Exposures (CVEs) affecting the organisation's iCS infrastructure.

Timely remediation of these CVEs is essential to reduce the risk of exploitation, prevent potential breaches, and maintain a strong security posture.

The progress section outlines the remediation progress for each identified vulnerability.

Addressing these findings promptly will significantly enhance your organisation's overall resilience against current and emerging threats.

Remediation Actions

Engineering teams are required to update to the latest version of Linux patches:

Test Case	Vulnerability Rating	Status
Log File Can be Downloaded by Anyone	Medium	Resolved
Passwords in /etc/passwd and MDS hashed	Medium	Resolved
Cleartext of Credentials in JS Files	Medium	Fix scheduled for Q2/25
Oracle Linux 8: bind/ and/ dhcp (ELSA-2024-1782)	Medium	Resolved
Oracle Linux 8: container-tools:ol8 (ELSA-2024-	Medium	Resolved

2098)		
Oracle Linux 8: curl (ELSA-2024-1601)	Medium	Resolved
Oracle Linux 8: edk2 (ELSA-2024-12343)	Medium	Resolved
Oracle Linux 8: expat (ELSA-2024-1615)	Medium	Resolved
Oracle Linux 8: glibc (ELSA-2024-2722)	Medium	Resolved
Oracle Linux 8: kvm_utils3 (ELSA-2023-12855)	Medium	Function made optional
Oracle Linux 8: less (ELSA-2024-1610)	Medium	Resolved
Oracle Linux 8: nodejs:18 (ELSA-2024-1510)	Medium	Resolved
Oracle Linux 8: open-vm-tools (ELSA-2023-7265)	Medium	Resolved
Oracle Linux 8: podman (ELSA-2024-12191)	Medium	Resolved
Oracle Linux 8: unbound (ELSA-2024-1751)	Medium	Resolved
Oracle Linux 8 / 9: Unbreakable Enterprise kernel (ELSA-2024-12255)	Medium	Resolved
Oracle MySOL Connectors (October 2023 CPU)	Medium	Resolved
Oracle MySOL Connectors C++ and ODBC (January 2024 CPU)	Medium	Resolved
SSH Terrapin Prefix Truncation Weakness (CVE-2023-48795)	Medium	Resolved
TLS cookie without secure flag set	Medium	Fix scheduled for Q4/25
Insecure Busybox Implementation in Hosts	Low	Future Roadmap
Password Complexity Didn't Meet Standard	Low	Resolved – Via configuration change
Unrestricted file upload	Low	Resolved
Vulnerable 3rd-party Dependencies	Low	Future Roadmap
Admin WebSocket Allows Insecure Transmission	Low	Future Roadmap
Cookie without HttpOnly flag set	Low	Future Roadmap
Cross-origin resource sharing: arbitrary origin trusted	Low	Future Roadmap
Insufficient Brute Force Attack Protection	Low	Resolved
Software Version Numbers Revealed	Low	Future Roadmap
Strict transport security not enforced	Low	Future Roadmap
Terminal Services Doesn’t	Low	Resolved – Via configuration

Use Network Level Authentication (NLA) only		change
Unprotected VoIP	Low	Future Roadmap
Web Server Allows Password Auto-Completion	Low	Resolved
Insecure Tools Installed on Boxes	Low	N/A
ICMP Timestamp Request Remote Date Disclosure	Low	Resolved
SSH Server CBC Mode Ciphers Enabled	Low	Resolved
SSH Weak Key Exchange Algorithms Enabled	Low	Resolved

Next Steps:

Please ensure you are up to date with the latest Speakerbus software, Lunix package updates and recommended configuration items. Speakerbus will provided updates when future fixes are available.

If you have any questions regarding this communication, please contact Speakerbus Global Customer Support (https://www.speakerbus.com/helpdesk).

End of Security Advisory.