Speakerbus

Title	SA-019 - External Penetration test (September 2024) remediation report
Security Advisory Number	Various
Affected Product(s)	QORUS Infrastructure
TAC Reference	N/A
Audience	Operations, Clients, Partners
Date	14 November 2024
Supersede	N/A
Severity	High / Medium

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:

High Impact Vulnerabilities in the report all are resolved:
CVE-2023-27522 - fixed in linux.oracle.com | ELSA-2023-5050
CVE-2023-25690 – fixed in linux.oracle.com | ELSA-2023-5050
CVE-2021-39275 – fixed in linux.oracle.com | ELSA-2022-0891
CVE-2022-23943 - fixed in linux.oracle.com | ELSA-2022-7647
CVE-2021-44790 – fixed in linux.oracle.com | ELSA-2022-0258
CVE-2022-31813 – fixed in linux.oracle.com | ELSA-2022-7647
CVE-2019-0211 – fixed in linux.oracle.com | ELSA-2019-0980
CVE-2019-10082 – fixed in linux.oracle.com | ELSA-2020-4751
CVE-2022-28615 – fixed in linux.oracle.com | ELSA-2022-7647
CVE-2022-36760 – fixed in linux.oracle.com | ELSA-2023-0852
CVE-2019-17567 – fixed in linux.oracle.com | ELSA-2020-4431

CVE-2022-30556 – fixed in linux.oracle.com | ELSA-2022-7647
CVE-2020-11993 – fixed in linux.oracle.com | ELSA-2021-1809

Medium Impact Vulnerabilities in the report all are resolved:
CVE-2022-22720 – fixed in linux.oracle.com | ELSA-2022-1049
CVE-2020-11984 - fixed in linux.oracle.com | ELSA-2021-1809
CVE-2021- 26691- fixed in linux.oracle.com | ELSA-2021-3816
CVE-2024- 27316 - fixed in linux.oracle.com | ELSA-2024-1786
CVE-2021-40438 - fixed in linux.oracle.com | ELSA-2021-3816
CVE-2024-38472 - fixed in linux.oracle.com | ELSA-2024-9573
CVE-2023-31122 - fixed in linux.oracle.com | ELSA-2024-3121
CVE-2023-45802 - fixed in linux.oracle.com | ELSA-2024-3121
CVE-2024-39573 - fixed in linux.oracle.com | ELSA-2024-4720
CVE-2021-44224 - fixed in linux.oracle.com | ELSA-2022-1915
CVE-2019-0217 - fixed in linux.oracle.com | ELSA-2019-3436
CVE-2019-0215 - fixed in linux.oracle.com | ELSA-2019-0980
CVE-2022-22721 - fixed in linux.oracle.com | ELSA-2019-0980
CVE-2024-38476 - fixed in linux.oracle.com | ELSA-2024-5193
CVE-2024-38473 – fixed in linux.oracle.com | ELSA-2024-4720
CVE-2024-38474 - fixed in linux.oracle.com | ELSA-2024-4720
CVE-2024-38477 - fixed in linux.oracle.com | ELSA-2024-4720
CVE-2022-28330 – OL 8 Not impacted (CVE-2022-28330)
CVE-2019-0196 - OL 8 Not impacted CVE-2019-0190
CVE-2021-26690 - fixed in linux.oracle.com | ELSA-2021-4257
CVE-2019-0196 - fixed in linux.oracle.com | ELSA-2020-4751
CVE-2022-30522 – fixed in linux.oracle.com | ELSA-2022-7647
CVE-2019-0197 - fixed in linux.oracle.com | ELSA-2020-4751

Diffie-Hellman Ephemeral Key Exchange – Updated in our latest server hardening guide.

SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Exchange – Updated to TLSv1.3 in our latest server hardening guide.

Next Steps:

To be resolved:

- SSL Cookie Without Secure Flag Set- Added to our development backlog, planned fix for Q3 2025.

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

End of Security Advisory.