SSA-170375: Multiple Vulnerabilities in RUGGEDCOM ROS before V5.9

Publication Date: 2024-07-09
Last Update: 2024-07-09
Current Version: V1.0
CVSS v3.1 Base Score: 8.8
CVSS v4.0 Base Score: 8.7

SUMMARY

Multiple vulnerabilities affect the RUGGEDCOM Operating System (ROS). The common denominator to all vulnerabilities is the leak of confidential information.

Siemens is preparing fix versions and recommends countermeasures for products where fixes are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM ROS V4.X family:	See below See further recommendations from section Workarounds and Mitigations
RUGGEDCOM i800: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS V4.X NC products:	See below See further recommendations from section Workarounds and Mitigations
RUGGEDCOM i800NC: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM i801NC: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM i802NC: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM i803NC: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM M2100NC: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM M2200NC: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM M969NC: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RMC30NC: All versions < V4.3.10 affected by CVE-2023-52237, CVE-2024-39675	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RMC8388NC V4.X: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RP110NC: All versions < V4.3.10 affected by CVE-2023-52237, CVE-2024-39675	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS1600FNC: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RS1600NC: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS1600TNC: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS400NC: All versions < V4.3.10 affected by CVE-2023-52237, CVE-2024-39675	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS401NC: All versions < V4.3.10 affected by CVE-2023-52237, CVE-2024-39675	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416NC: All versions < V4.3.10 affected by CVE-2023-52237, CVE-2024-39675	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416NCv2 V4.X: All versions < V4.3.10 affected by CVE-2023-52237, CVE-2024-39675	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416PNC: All versions < V4.3.10 affected by CVE-2023-52237, CVE-2024-39675	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416PNCv2 V4.X: All versions < V4.3.10 affected by CVE-2023-52237, CVE-2024-39675	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RS8000ANC: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000HNC: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000NC: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000TNC: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900GNC: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900GNC(32M) V4.X: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900GPNC: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900LNC: All versions affected by CVE-2023-52237	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900MNC-GETS-C01: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RS900MNC-GETS-XX: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900MNC-STND-XX: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900MNC-STND-XX-C01: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900NC: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900NC(32M) V4.X: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS910LNC: All versions affected by CVE-2023-52237, CVE-2024-39675	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS910NC: All versions < V4.3.10 affected by CVE-2023-52237, CVE-2024-39675	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS920LNC: All versions affected by CVE-2023-52237, CVE-2024-39675	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS930LNC: All versions affected by CVE-2023-52237	Currently no fix is planned See recommendations from section Workarounds and Mitigations

RUGGEDCOM RS940GNC: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS969NC: All versions affected by CVE-2023-52237	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100NC: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100NC(32M) V4.X: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100PNC: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2200NC: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2288NC V4.X: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300NC V4.X: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300PNC V4.X: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RSG2488NC V4.X: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG920PNC V4.X: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM i801: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM i802: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM i803: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM M2100: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM M2200: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM M969: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RMC30: All versions < V4.3.10 affected by CVE-2023-52237, CVE-2024-39675	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RMC8388 V4.X: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RP110: All versions < V4.3.10 affected by CVE-2023-52237, CVE-2024-39675	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS1600: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS1600F: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS1600T: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS400: All versions < V4.3.10 affected by CVE-2023-52237, CVE-2024-39675	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS401: All versions < V4.3.10 affected by CVE-2023-52237, CVE-2024-39675	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RS416: All versions < V4.3.10 affected by CVE-2023-52237, CVE-2024-39675	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416P: All versions < V4.3.10 affected by CVE-2023-52237, CVE-2024-39675	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416Pv2 V4.X: All versions < V4.3.10 affected by CVE-2023-52237, CVE-2024-39675	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416v2 V4.X: All versions < V4.3.10 affected by CVE-2023-52237, CVE-2024-39675	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000A: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000H: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000T: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RS900: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900 (32M) V4.X: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900G: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900G (32M) V4.X: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900GP: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900L: All versions affected by CVE-2023-52237	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900M-GETS-C01: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900M-GETS-XX: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900M-STND-C01: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RS900M-STND-XX: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900W: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS910: All versions < V4.3.10 affected by CVE-2023-52237, CVE-2024-39675	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS910L: All versions affected by CVE-2023-52237, CVE-2024-39675	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS910W: All versions < V4.3.10 affected by CVE-2023-52237, CVE-2024-39675	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS920L: All versions affected by CVE-2023-52237, CVE-2024-39675	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS920W: All versions affected by CVE-2023-52237, CVE-2024-39675	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS930L: All versions affected by CVE-2023-52237	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS930W: All versions affected by CVE-2023-52237	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS940G: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RS969: All versions affected by CVE-2023-52237	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100 (32M) V4.X: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100P: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2200: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2288 V4.X: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300 V4.X: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300P V4.X: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2488 V4.X: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RSG920P V4.X: All versions < V4.3.10 affected by CVE-2023-52237	Update to V4.3.10 or later version https://support.industry.siemens.com/cs/ww/en/view/109972218/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS V5.X family:	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RMC8388 V5.X: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2024-38278	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM ROS V5.X NC products:	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RMC8388NC V5.X: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2024-38278	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416NCv2 V5.X: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2024-38278, CVE-2024-39675	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416PNCv2 V5.X: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2024-38278, CVE-2024-39675	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900GNC(32M) V5.X: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2024-38278	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RS900NC(32M) V5.X: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2024-38278	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100NC(32M) V5.X: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2024-38278	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2288NC V5.X: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2024-38278	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300NC V5.X: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2024-38278	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300PNC V5.X: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2024-38278	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2488NC V5.X: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2024-38278	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG920PNC V5.X: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2024-38278	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSL910NC: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2024-38278	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RS416Pv2 V5.X: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2024-38278, CVE-2024-39675	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416v2 V5.X: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2024-38278, CVE-2024-39675	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900 (32M) V5.X: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2024-38278	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900G (32M) V5.X: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2024-38278	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100 (32M) V5.X: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2024-38278	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2288 V5.X: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2024-38278	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300 V5.X: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2024-38278	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300P V5.X: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2024-38278	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RSG2488 V5.X: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2024-38278	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG907R: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2024-38278	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG908C: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2024-38278	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG909R: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2024-38278	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG910C: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2024-38278	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG920P V5.X: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2024-38278	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSL910: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2024-38278	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RST2228: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2023-52238, CVE-2024-38278	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RST2228P: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2023-52238, CVE-2024-38278	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RST916C: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2024-38278	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RST916P: All versions < V5.9.0 affected by CVE-2023-52237, CVE-2024-38278	Update to V5.9.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109972217/ See further recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- For CVE-2023-52237, CVE-2023-52238: Disable the webserver if not required on the affected systems. Restrict the access to Port 80/tcp and 443/tcp to trusted IP address only
- For CVE-2024-38278: Disable the IP Forwarding if not required on the affected system. Also note, the IP forwarding is disabled by default
- For CVE-2024-39675: Disable the Modbus Server if not required on the affected system. Restrict the access to Port 502/tcp to trusted IP address only. Also note, Modbus is disabled by default

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals. Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

RUGGEDCOM ROS-based devices, typically switches and serial-to-Ethernet devices, are used to connect devices that operate in harsh environments such as electric utility substations and traffic control cabinets.

VULNERABILITY DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

Vulnerability CVE-2023-52237

The web server of the affected devices allow a low privileged user to access hashes and password salts of all system's users, including admin users. An attacker could use the obtained information to brute force the passwords offline.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CVSS v4.0 Base Score	7.7
CVSS Vector	CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2023-52238

The web server of the affected systems leaks the MACSEC key in clear text to a logged in user. An attacker with the credentials of a low privileged user could retrieve the MACSEC key and access (decrypt) the ethernet frames sent by authorized recipients.

CVSS v3.1 Base Score	4.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CVSS v4.0 Base Score	2.3
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2024-38278

The affected products with IP forwarding enabled wrongly make available certain remote services in non-managed VLANs, even if these services are not intentionally activated. An attacker could leverage this vulnerability to create a remote shell to the affected system.

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CVSS v4.0 Base Score	7.5
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:P/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-266: Incorrect Privilege Assignment

Vulnerability CVE-2024-39675

In some configurations the affected products wrongly enable the Modbus service in non-managed VLANS. Only serial devices are affected by this vulnerability.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Stephen Craven for reporting the vulnerabilities CVE-2024-38278 and CVE-2024-39675
- Thomas Riedmaier from Siemens Energy for reporting the vulnerabilities CVE-2023-52237, CVE-2023-52238

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2024-07-09): Publication Date

TERMS OF USE