SSA-256353: Third-Party Component Vulnerabilities in RUGGEDCOM ROS

Publication Date: 2022-03-08
Last Update: 2023-12-12
Current Version: V1.5
CVSS v3.1 Base Score: 9.6

SUMMARY

Multiple vulnerabilities affect various third-party components of the RUGGEDCOM Operating System (ROS). If exploited, an attacker could cause a denial-of-service, act as a man-in-the-middle or retrieval of sensitive information or gain privileged functions.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM i800: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM i800NC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM i801: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM i801NC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM i802: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM i802NC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM i803: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM i803NC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM M969: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM M969F: All versions affected by CVE-2021-37208, CVE-2021-42016, CVE-2021-42017, CVE-2021-42018, CVE-2021-42019	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM M969NC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM M2100: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM M2100F: All versions affected by CVE-2021-37208, CVE-2021-42016, CVE-2021-42017, CVE-2021-42018, CVE-2021-42019	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM M2100NC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM M2200: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM M2200F: All versions affected by CVE-2021-37208, CVE-2021-42016, CVE-2021-42017, CVE-2021-42018, CVE-2021-42019	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM M2200NC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RMC30: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RMC30NC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RMC8388 V4.X: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RMC8388 V5.X: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RMC8388NC V4.X: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RMC8388NC V5.X: All versions < V5.6.0 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RP110: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RP110NC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS400: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS400F: All versions affected by CVE-2021-37208, CVE-2021-42016, CVE-2021-42017, CVE-2021-42018, CVE-2021-42019	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS400NC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS401: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS401NC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416F: All versions affected by CVE-2021-37208, CVE-2021-42016, CVE-2021-42017, CVE-2021-42018, CVE-2021-42019	Currently no fix is planned See recommendations from section Workarounds and Mitigations

RUGGEDCOM RS416NC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416NCv2 V4.X: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416NCv2 V5.X: All versions < V5.6.0 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416P: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416PF: All versions affected by CVE-2021-37208, CVE-2021-42016, CVE-2021-42017, CVE-2021-42018, CVE-2021-42019	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416PNC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416PNCv2 V4.X: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416PNCv2 V5.X: All versions < V5.6.0 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416Pv2 V4.X: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RS416Pv2 V5.X: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416v2 V4.X: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416v2 V5.X: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900 (32M) V4.X: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900 (32M) V5.X: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900F: All versions affected by CVE-2021-37208, CVE-2021-42016, CVE-2021-42017, CVE-2021-42018, CVE-2021-42019	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900G: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900G (32M) V4.X: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RS900G (32M) V5.X: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900GF: All versions affected by CVE-2021-37208, CVE-2021-42016, CVE-2021-42017, CVE-2021-42018, CVE-2021-42019	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900GNC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900GNC(32M) V4.X: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900GNC(32M) V5.X: All versions < V5.6.0 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900GP: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900GPF: All versions affected by CVE-2021-37208, CVE-2021-42016, CVE-2021-42017, CVE-2021-42018, CVE-2021-42019	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900GPNC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900L: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RS900LNC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900M-GETS-C01: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900M-GETS-XX: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900M-STND-C01: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900M-STND-XX: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900MNC-GETS-C01: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900MNC-GETS-XX: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900MNC-STND-XX: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RS900MNC-STND-XX-C01: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900NC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900NC(32M) V4.X: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900NC(32M) V5.X: All versions < V5.6.0 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900W: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS910: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS910L: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS910LNC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RS910NC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS910W: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS920L: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS920LNC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS920W: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS930L: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS930LNC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS930W: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RS940G: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS940GF: All versions affected by CVE-2021-37208, CVE-2021-42016, CVE-2021-42017, CVE-2021-42018, CVE-2021-42019	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS940GNC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS969: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS969NC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS1600: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS1600F: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS1600FNC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS1600NC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RS1600T: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS1600TNC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000A: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000ANC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000H: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000HNC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000NC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RS8000T: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000TNC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG907R: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG908C: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG909R: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG910C: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG920P V4.X: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG920P V5.X: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RSG920PNC V4.X: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG920PNC V5.X: All versions < V5.6.0 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100 (32M) V4.X: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100 (32M) V5.X: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100F: All versions affected by CVE-2021-37208, CVE-2021-42016, CVE-2021-42017, CVE-2021-42018, CVE-2021-42019	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100NC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100NC(32M) V4.X: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100NC(32M) V5.X: All versions < V5.6.0 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RSG2100P: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100PF: All versions affected by CVE-2021-37208, CVE-2021-42016, CVE-2021-42017, CVE-2021-42018, CVE-2021-42019	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100PNC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2200: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2200F: All versions affected by CVE-2021-37208, CVE-2021-42016, CVE-2021-42017, CVE-2021-42018, CVE-2021-42019	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2200NC: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2288 V4.X: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2288 V5.X: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2288NC V4.X: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RSG2288NC V5.X: All versions < V5.6.0 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300 V4.X: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300 V5.X: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300F: All versions affected by CVE-2021-37208, CVE-2021-42016, CVE-2021-42017, CVE-2021-42018, CVE-2021-42019	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300NC V4.X: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300NC V5.X: All versions < V5.6.0 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300P V4.X: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300P V5.X: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300PF: All versions affected by CVE-2021-37208, CVE-2021-42016, CVE-2021-42017, CVE-2021-42018, CVE-2021-42019	Currently no fix is planned See recommendations from section Workarounds and Mitigations

RUGGEDCOM RSG2300PNC V4.X: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300PNC V5.X: All versions < V5.6.0 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2488 V4.X: All versions < V4.3.8	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2488 V5.X: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2488F: All versions affected by CVE-2021-37208, CVE-2021-42016, CVE-2021-42017, CVE-2021-42018, CVE-2021-42019	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2488NC V4.X: All versions < V4.3.8 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V4.3.8 or later version https://support.industry.siemens.com/cs/ww/en/view/109816735/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2488NC V5.X: All versions < V5.6.0 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSL910: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSL910NC: All versions < V5.6.0 affected by CVE-2021-37208, CVE-2021-42018, CVE-2021-42019, CVE-2021-42020	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RST916C: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RST916P: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RST2228: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RST2228P: All versions < V5.6.0	Update to V5.6.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109806156/ 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:

- Restrict web server access in affected system(s) to ports 443/TCP and 22/TCP, to trusted IP addresses only
- Restrict access to port 69/UDP to trusted IP addresses only, for the TFTP vulnerability

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 CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2021-37208

Improper neutralization of special characters on the web server configuration page could allow an attacker, in a privileged position, to retrieve sensitive information via cross-site scripting.

CVSS v3.1 Base Score	9.6
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:H/A:H/E:P/RL:T/RC:C
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Vulnerability CVE-2021-42016

A timing attack, in a third-party component, could make the retrieval of the private key possible, used for encryption of sensitive data.

If a threat actor were to exploit this, the data integrity and security could be compromised.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-208: Observable Timing Discrepancy

Vulnerability CVE-2021-42017

A new variant of the POODLE attack has left a third-party component vulnerable due to the implementation flaws of the CBC encryption mode in TLS 1.0 to 1.2.

If an attacker were to exploit this, they could act as a man-in-the-middle and eavesdrop on encrypted communications.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-358: Improperly Implemented Security Check for Standard

Vulnerability CVE-2021-42018

Within a third-party component, whenever memory allocation is requested, the out of bound size is not checked.

Therefore, if size exceeding the expected allocation is assigned, it could allocate a smaller buffer instead. If an attacker were to exploit this, they could cause a heap overflow.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2021-42019

Within a third-party component, the process to allocate partition size fails to check memory boundaries.

Therefore, if a large amount is requested by an attacker, due to an integer-wrap around, it could result in a small size being allocated instead.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2021-42020

The third-party component, in its TFTP functionality fails to check for null terminations in file names.

If an attacker were to exploit this, it could result in data corruption, and possibly a hard-fault of the application.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-754: Improper Check for Unusual or Exceptional Conditions

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Siemens Energy for coordinated disclosure of CVE-2021-37208

ADDITIONAL INFORMATION

On FIPS devices, if the TFTP feature is turned on, it is no longer considered to be in FIPS mode and considered as regular ROS device (described in FIPS user manual)

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 (2022-03-08):	Publication Date
V1.1 (2022-03-11):	Corrected the list of affected products and fix releases
V1.2 (2022-04-12):	Added acknowledgements
V1.3 (2023-03-14):	Corrected the list of affected products and added fix for V4.3.8
V1.4 (2023-04-11):	Added multiple missing affected products (only affected by CVE-2021-37208, CVE-2021-42016, CVE-2021-42017, CVE-2021-42018 and CVE-2021-42019) with no fix currently planned
V1.5 (2023-12-12):	Added missing affected products: RUGGEDCOM RS416NCv2 V4.X, RUGGEDCOM RS416PNCv2 V4.x, RUGGEDCOM RS416v2 V4.X, RUGGEDCOM RS416Pv2 V4.X. Adjusted the name of RUGGEDCOM RS416NCv2 V5.X, RUGGEDCOM RS416PNCv2 V5.x, RUGGEDCOM RS416v2 V5.X, RUGGEDCOM RS416Pv2 V5.X (added reference to V5.X). Added Additional note for FIPS devices

TERMS OF USE