

SSA-908185: Mirror Port Isolation Vulnerability in RUGGEDCOM ROS Devices

Publication Date: 2023-08-08
Last Update: 2023-11-14
Current Version: V1.1
CVSS v3.1 Base Score: 9.1

SUMMARY

A vulnerability was identified in RUGGEDCOM ROS devices with mirror port enabled, that could allow an attacker to inject information into the network via the mirror port.

Siemens has released updates for several affected products and recommends to update to the latest versions. Siemens is preparing further updates and recommends specific countermeasures for products where updates are not, or not yet available.

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	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	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	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	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	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM M969NC: 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 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	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM M2100NC: 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 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	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM M2200NC: 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 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	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 < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RMC8388NC 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 RMC8388NC V5.X: All versions < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ 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	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	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS400F: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS400NC: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS401: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS401NC: All versions	Currently no fix is planned See 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	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416NC: 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 RS416NCv2 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 RS416NCv2 V5.X: All versions < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ 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	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS416PNC: 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 RS416PNCv2 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 RS416PNCv2 V5.X: All versions < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ 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 < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ 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 < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900: All versions with switch chip M88E6083	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900: All versions < V4.3.8 except for switch chip M88E6083	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 < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900F: All versions	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 < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900GF: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900GNC: 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 RS900GNC(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 RS900GNC(32M) V5.X: All versions < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ 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	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900GPNC: 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 RS900L: All versions with switch chip M88E6083	Currently no fix is planned See recommendations from section Workarounds and Mitigations

RUGGEDCOM RS900L: All versions < V4.3.8 except for switch chip M88E6083	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 with switch chip M88E6083	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900LNC: All versions < V4.3.8 except for switch chip M88E6083	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	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	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	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	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 with switch chip M88E6083	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS900NC: All versions < V4.3.8 except for switch chip M88E6083	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	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 < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ 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	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	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	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	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	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS940GNC: 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 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	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	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS1600F: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS1600FNC: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS1600NC: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations

RUGGEDCOM RS1600T: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS1600TNC: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000A: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000ANC: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000H: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000HNC: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000NC: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000T: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RS8000TNC: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG907R: All versions < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RSG908C: All versions < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG909R: All versions < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG910C: All versions < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ 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 < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG920PNC 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 RSG920PNC V5.X: All versions < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ 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 < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100F: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100NC: 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 RSG2100NC(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 RSG2100NC(32M) V5.X: All versions < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ 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	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2100PNC: 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 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	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2200NC: 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 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 < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2288NC 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 RSG2288NC V5.X: All versions < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ 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 < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RSG2300F: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300NC 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 RSG2300NC V5.X: All versions < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ 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 < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300PF: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2300PNC 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 RSG2300PNC V5.X: All versions < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ 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 < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2488F: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
RUGGEDCOM RSG2488NC 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 RSG2488NC V5.X: All versions < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSL910: All versions < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RSL910NC: All versions < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RST916C: All versions < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RST916P: All versions < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ See further recommendations from section Workarounds and Mitigations
RUGGEDCOM RST2228: All versions < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ See further recommendations from section Workarounds and Mitigations

RUGGEDCOM RST2228P: All versions < V5.8.0	Update to V5.8.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824855/ 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:

- Configure ingress filtering to control traffic flow when port mirroring is enabled:
 - Enable Ingress Filtering
 - Disabled RSTP on the Target port(s)
 - Disable Neighbor Discovery protocol on the target port(s)
 - Disable LLDP on the target port(s)
- Further details can be find at <https://support.industry.siemens.com/cs/ww/en/view/109759351>

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-2023-24845

The affected products insufficiently block data from being forwarded over the mirror port into the mirrored network.

An attacker could use this behavior to transmit malicious packets to systems in the mirrored network, possibly influencing their configuration and runtime behavior.

CVSS v3.1 Base Score	9.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-684: Incorrect Provision of Specified Functionality

ADDITIONAL INFORMATION

The fix for RS900 devices (see full list below) doesn't apply for devices using the M88E6083 chip. To check which chip is used by your RS900 device:

1. Login to the device via the local console, SSH, or telnet (for NC class devices) with the administrator credentials
2. Enter the interactive shell by using the hot-key "Ctrl-S"
3. Enter the factory mode by typing the "factory" command, and follow the prompts to login.
4. Enter the command "m88e6 globals"

If the output contains the text "M88E6083", then the device is unable to be patched (see WORKAROUNDS AND MITIGATIONS section). Otherwise, the device can be patched with the firmware version identified in the AFFECTED PRODUCTS AND SOLUTION table above.

List of RS900 devices:

- RUGGEDCOM RS900
- RUGGEDCOM RS900L
- RUGGEDCOM RS900LNC
- RUGGEDCOM RS900NC

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 (2023-08-08):	Publication Date
V1.1 (2023-11-14):	Added fix to all V5.X products. 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 fix for RS416*NC V4.X

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.