

## SSA-764417: Weak Encryption Vulnerability in RUGGEDCOM ROS Devices

Publication Date: 2022-03-08  
Last Update: 2023-11-14  
Current Version: V1.8  
CVSS v3.1 Base Score: 6.7

### SUMMARY

The SSH server on RUGGEDCOM ROS devices is configured to offer weak ciphers by default. This could allow an unauthorized attacker in a man-in-the-middle position to read and modify any data passed over the connection between legitimate clients and the affected device.

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 <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM i801: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM i802: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM i803: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM M969: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>

RUGGEDCOM M2100: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM M2200: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RMC30: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RMC8388 V4.X: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RMC8388 V5.X: All versions < V5.7.0	Update to V5.7.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109814608/">https://support.industry.siemens.com/cs/ww/en/view/109814608/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RP110: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS400: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS401: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>

RUGGEDCOM RS416: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS416P: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS416Pv2 V4.X: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS416Pv2 V5.X: All versions < V5.7.0	Update to V5.7.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109814608/">https://support.industry.siemens.com/cs/ww/en/view/109814608/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS416v2 V4.X: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS416v2 V5.X: All versions < V5.7.0	Update to V5.7.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109814608/">https://support.industry.siemens.com/cs/ww/en/view/109814608/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS900: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS900 (32M) V4.X: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>

RUGGEDCOM RS900 (32M) V5.X: All versions < V5.7.0	Update to V5.7.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109814608/">https://support.industry.siemens.com/cs/ww/en/view/109814608/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS900G: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS900G (32M) V4.X: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS900G (32M) V5.X: All versions < V5.7.0	Update to V5.7.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109814608/">https://support.industry.siemens.com/cs/ww/en/view/109814608/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS900GP: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS900L: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS900M-GETS-C01: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS900M-GETS-XX: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>

RUGGEDCOM RS900M-STND-C01: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS900M-STND-XX: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS900W: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS910: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS910L: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS910W: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS920L: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS920W: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>

RUGGEDCOM RS930L: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS930W: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS940G: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS969: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS1600: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS1600F: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS1600T: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS8000: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>

RUGGEDCOM RS8000A: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS8000H: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RS8000T: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RSG907R: All versions < V5.7.0	Update to V5.7.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109814608/">https://support.industry.siemens.com/cs/ww/en/view/109814608/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RSG908C: All versions < V5.7.0	Update to V5.7.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109814608/">https://support.industry.siemens.com/cs/ww/en/view/109814608/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RSG909R: All versions < V5.7.0	Update to V5.7.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109814608/">https://support.industry.siemens.com/cs/ww/en/view/109814608/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RSG910C: All versions < V5.7.0	Update to V5.7.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109814608/">https://support.industry.siemens.com/cs/ww/en/view/109814608/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RSG920P V4.X: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>

RUGGEDCOM RSG920P V5.X: All versions < V5.7.0	Update to V5.7.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109814608/">https://support.industry.siemens.com/cs/ww/en/view/109814608/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RSG2100: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RSG2100 (32M) V4.X: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RSG2100 (32M) V5.X: All versions < V5.7.0	Update to V5.7.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109814608/">https://support.industry.siemens.com/cs/ww/en/view/109814608/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RSG2100P: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RSG2200: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RSG2288 V4.X: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RSG2288 V5.X: All versions < V5.7.0	Update to V5.7.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109814608/">https://support.industry.siemens.com/cs/ww/en/view/109814608/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>

RUGGEDCOM RSG2300 V4.X: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RSG2300 V5.X: All versions < V5.7.0	Update to V5.7.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109814608/">https://support.industry.siemens.com/cs/ww/en/view/109814608/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RSG2300P V4.X: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RSG2300P V5.X: All versions < V5.7.0	Update to V5.7.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109814608/">https://support.industry.siemens.com/cs/ww/en/view/109814608/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RSG2488 V4.X: All versions < V4.3.8	Update to V4.3.8 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109816735/">https://support.industry.siemens.com/cs/ww/en/view/109816735/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RSG2488 V5.X: All versions < V5.7.0	Update to V5.7.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109814608/">https://support.industry.siemens.com/cs/ww/en/view/109814608/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RSL910: All versions < V5.7.0	Update to V5.7.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109814608/">https://support.industry.siemens.com/cs/ww/en/view/109814608/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RST916C: All versions < V5.7.0	Update to V5.7.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109814608/">https://support.industry.siemens.com/cs/ww/en/view/109814608/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>

RUGGEDCOM RST916P: All versions < V5.7.0	Update to V5.7.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109814608/">https://support.industry.siemens.com/cs/ww/en/view/109814608/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RST2228: All versions < V5.7.0	Update to V5.7.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109814608/">https://support.industry.siemens.com/cs/ww/en/view/109814608/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>
RUGGEDCOM RST2228P: All versions < V5.7.0	Update to V5.7.0 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109814608/">https://support.industry.siemens.com/cs/ww/en/view/109814608/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>

## **WORKAROUNDS AND MITIGATIONS**

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

- Configure the SSH clients to make use of the following strong key exchange ciphers, supported by the ROS SSH server: ecdh-sha2-nistp256, ecdh-sha2-nistp384, or ecdh-sha2-nistp521
- Add only trusted SSH client public keys to ROS and allow access to those clients only

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-2021-37209**

The SSH server on affected devices is configured to offer weak ciphers by default.

This could allow an unauthorized attacker in a man-in-the-middle position to read and modify any data passed over the connection between legitimate clients and the affected device.

CVSS v3.1 Base Score	6.7
CVSS Vector	<a href="#">CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:H/A:H/E:P/RL:U/RC:C</a>
CWE	CWE-326: Inadequate Encryption Strength

## **ACKNOWLEDGMENTS**

Siemens thanks the following party for its efforts:

- Michael Messner from Siemens Energy for reporting the vulnerability

## **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 (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 (2022-06-14):	Corrected title, vulnerability description, CVSS vector and CWE ID; clarified that a fix release is currently not available for affected devices
V1.4 (2022-08-09):	Reflected a more accurate fix status in advisory
V1.5 (2022-11-08):	Reflect information about an upcoming fix. Highlight version lines of the affected devices
V1.6 (2022-12-13):	Added fix for RUGGEDCOM ROS V5.X devices
V1.7 (2023-03-14):	Added missing affected products. Added fix for RUGGEDCOM ROS devices using V4.X
V1.8 (2023-11-14):	Added missing affected products: RUGGEDCOM RS416v2 V4.X, RUGGEDCOM RS416Pv2 V4.X. Adjusted the name of RUGGEDCOM RS416v2 V5.X, RUGGEDCOM RS416Pv2 V5.X (added reference to V5.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](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.