Field Bulletin #: FB011

Date of Notice: July 22, 2021

Issue: SureLine® Vulnerability

Affected Product(s): All versions of Longport, RICI, Ventnor, Margate, Brigantine SGP, SGP

Affected Software Revision(s): SureLine® software v8.7.0 or older

Problem Description:

In the SureLine application software used on Sunhillo communication appliances, v8.7.0 and older, a vulnerability was discovered that allows unauthenticated operating system (OS) command injection making it possible for an attacker to execute arbitrary commands with root privileges using the browser interface. This vulnerability has been disclosed under CVE-2021-36380.

Analysis:

The SureLine Network Diagnostic menu items execute shell commands directly without first checking the user input allowing an attacker to execute malicious code.

Resolution:

When this vulnerability was discovered, Sunhillo performed a full code inspection of all user inputs into the Web GUI and fixed all incidents of direct shell injection from the web GUI. These fixes are released in v8.7.0.1.1 (branch) and versions v8.7.1 and greater.

Sunhillo is updating its internal coding standards to include more secure coding practices to prevent these types of vulnerabilities in the future.

Recommended Action:

For SureLine-based products, Sunhillo recommends our customers upgrade to at least v8.7.0.1.1, v8.7.1 or higher.