Stephenson Stellar Corporation

Title: Senior Vulnerability Researcher **Position ID:** 2026-0008	**Type Position:** Full Time **Level:** PL4
Primary Location: To be determined	**Travel Required:** 20% CONUS and HI
Alternate Location: Home office anywhere in USA	**Contact:** Technical: aechevarria@stephensonstellar.org (Axel Echevarria) Human Resource: bmoyer@stephensonstellar.org (Barb Moyer)

Company Background: Stephenson Stellar Corporation (Stellar) is a nonprofit research and development organization focused on assuring our nation remains a global leader in the Space Domain. Our mission is to foster technological innovation and provide secure space-based solutions.

Stellar is an equal opportunity employer, and all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, national origin, age, disability status, protected veteran status, or any other characteristic protected by law.

Additional information at: www.stephensonstellar.org

Job Description: In this position, you will serve as a Senior Vulnerability Researcher for the Space Systems Protection Directorate. You will work alongside a multidisciplinary team of cybersecurity researchers and engineers supporting space and ground system security initiatives. This is a hands-on technical role where reverse engineering, exploit development, and creative problem-solving meet mission-critical impact. The candidate is to be passionate about uncovering vulnerabilities at the OS, application, and firmware levels, and crafting proof-of-concept exploits to validate findings and have a deep technical understanding of embedded Linux and real-time operating systems (RTOS). The position responsibilities include: (1) Perform vulnerability research and reverse engineering on embedded Linux and RTOS-based systems, including firmware and applications; (2) Conduct static and dynamic analysis of binaries and source code to identify security flaws and exploitation paths; (3) Develop proof-of-concept exploits and mitigations for discovered vulnerabilities; (4) Analyze BusyBox-based environments and other minimalized system configurations for misconfigurations and code-level weaknesses; and (5) Contribute to custom fuzzing and emulation environments for embedded targets (QEMU, Unicorn, etc.).

Requirements

Clearance: Ability to maintain a Top-Secret clearance.
Citizenship: Candidate must be a United States citizen.
Education:

- BS in Computer Science, Computer Engineering, Cybersecurity, Electrical Engineering.
- An advanced degree is preferred.

Experience:

- 7 plus years of progressive, hands-on experience in vulnerability assessment, penetration testing or reverse engineering.

Required Skills:

- Strong knowledge of: (1) Embedded Linux internals (kernel, drivers, IPC, memory management); (2) RTOS platforms (VxWorks, RTEMS, FreeRTOS, Integrity, etc.); (3) Reverse engineering tools (IDA Pro, Ghidra, Binary Ninja, radare2); (4) Exploit development techniques (heap/stack exploitation, ROP, sandbox bypass); (5) Firmware extraction and analysis (binwalk, Ghidra, QEMU, firmware unpackers); and (6) C/C++ and Python for tooling and exploit scripting.
- Experience with BusyBox utilities and lightweight Linux environments.
- Experience testing embedded systems, firmware, or devices is highly desirable (ground-station equipment, communications gear, RTOS-based firmware).
- Strong written and verbal communication skills; ability to present technical findings to non-technical leadership and to produce clear, prioritized remediation plans.
- Demonstrate ability and willingness to train, mentor, and develop junior or mid-level engineers in vulnerability research methodologies, fostering knowledge transfer and a culture of technical excellence.

Desired Skills:

- Experience with space vehicle software stacks (flight software, command & data handling, TT&C, payload management, etc.)
- Familiarity with radiation-hardened hardware, limited SWaP environments, or satellite emulation frameworks.
- Understanding of secure boot, hardware root of trust, and cryptographic modules (FIPS 140-2).
- Familiarity with electronic warfare, RF protocol analysis, SDR toolchains (GNU Radio, URH), or telecommand/telemetry exploitation techniques for ground systems.