E&M TECHNOLOGIES, INC.

E&M Technologies
4465 Northpark Drive, Suite 304
Colorado Springs, CO 80907

POSITION: Level 3 Vulnerability Researcher
Work Location: Annapolis Junction, MD
Required Clearance: TS/SCI with FS Poly

E&M Technologies, Inc. is currently seeking a **Level 2 Vulnerability Researcher** to support a Federal government client.

Required Skills/Experience:

- Lead efforts to debug software and troubleshoot issues with software crashes and programmatic flow
- Ability to perform source code analysis to discover software flaws, and provide/author documentation on the impact and severity of the flaw
- Ability to develop robust exploits (advancements beyond initial proof-of-concept such as version coverage, decreased failure rate, handling edge cases, etc.) against research targets, prototypes, and hands-on demonstrations of vulnerability analysis results
- Edit/Approve and participate in technical presentations on assigned projects
- Subject Matter Expert and Leader of at least one technology area responsible for reverse engineering and vulnerability analysis of hardware components, software applications, and operating systems to determine functionality, code structure, and circuit design for the use in the discovery of initial access capabilities
- Meet all qualifications of a CNO Vulnerability Researcher/Analyst II
- Proven results from participation in vulnerability discovery efforts within the last twelve (12) months
- Demonstrated ability to discover multiple previously unknown vulnerabilities (0-day) across multiple versions of similar technologies.
- Demonstrated ability to discover multiple previously unknown vulnerabilities (0-day) that ultimately achieve reliable remote code execution and/or reliable privilege escalation.

Desired Skills/Experience:

- Experience programming in Assembly, C, C#, C++, Perl, or Python with a focus on an understanding of system interactions with these libraries vs. production-style environments
- Use of Unix/Windows system API's
- Understanding of virtual function tables in C++
- Heap allocation strategies and protections
- Experience with very large software projects a plus
- Kernel programming experience (WDK / Unix||Linux) a significant plus
- Hardware/Software reverse engineering, which often includes the use of tools (e.g., IDA Pro, Ghidra, Binary Ninja) to identify abstract concepts about the code flow of an application

E&M TECHNOLOGIES, INC.

E&M Technologies
4465 Northpark Drive, Suite 304
Colorado Springs, CO 80907

- For Hardware reverse engineering, candidates expected to have performed analysis of embedded devices, focusing primarily on identifying the software stack and points of entry to the hardware (e.g. not interested in FPGA reverse engineering, or other circuit reverse engineering)
- Candidates who can merge low-level knowledge about compilation of C/C++ code with a nuanced understanding of system design to identify and exploit common vulnerability patterns
- Candidates should be comfortable with, at a minimum, user-mode stack-based buffer overflows, and heap-based exploitation strategies

Required Education:

- Bachelor's Degree in Computer Science or related field plus minimum three (3) years contiguous experience

E&M Technologies offers competitive salaries, medical benefits, and a 401k plan.

To Apply for this Position:
You must have the Required Qualifications in your resume to be selected as a candidate.

Send your resume to emtech@eandmtech.com

All qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, marital status, national origin, age, veteran status, disability, or any other protected class. U.S. Citizenship is required for most positions.