Computer Science / IT

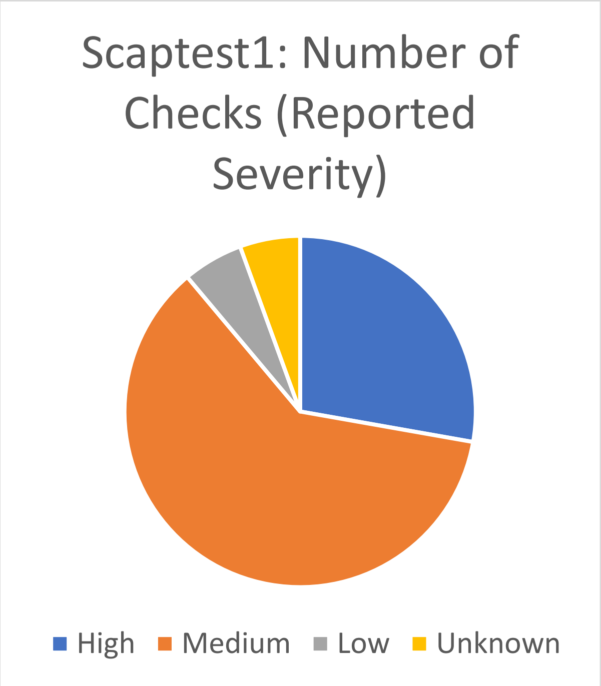
# Evaluating NCCS System Security Compliance

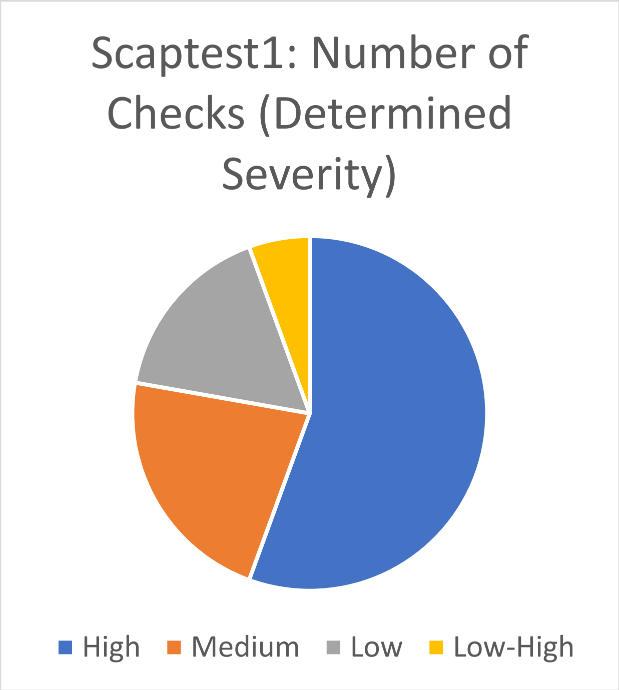
Aman Thanvi, George Rumney, John Jasen, Jasaun Neff, Jordan Caraballo-Vega

University of Maryland, College Park, University of Maryland College of Computer, Mathematical, and Natural Sciences, 2300 Symons Hall, 7998 Regents Dr, College Park, MD 20742

NASA Center for Climate Simulation, High Performance Computing Division, NASA Goddard Space Flight Center, Mail Code 606, Greenbelt, MD 20771

The objective of this project was to evaluate NCCS system security compliance using OpenSCAP, CIS, NASA, and other government and industry standards. Given two images deployed from an ADAPT OpenStack node, one CentOS 7 base image and one CentOS 7 NCCS hardened image, the task was to evaluate NCCS security compliance with the goal of improving NCCS security posture and missions and systems operations over time. The primary question addressed throughout the project was “what are the relative risks with respect to the compliance of NCCS’s systems and service stacks?” In addressing this question, NCCS’s underlying systems infrastructures and current security guidelines and posturing were evaluated. The main objective was to evaluate the degrees of systems compliance using OpenSCAP, CIS, NASA, and other government and industry standards, documentations, and guidelines. Given two OpenStack images, one CentOS 7 base image and one CentOS 7 NCCS hardened image, the task was to evaluate and analyze their security compliance with detailed, scored reports generated by the benchmarking tools by documenting flagged issues, determining the best course of action as to how to resolve them, assess the feasibility of the implementation of resolutions to known issues, and revise and improve preexisting baselines. Upon completing evaluation, many current checks needed revision; referencing best practices and policies put into place by government publications, like NIST’s 800 documentation, and more modern security documentation and guidelines, there were multiple risk areas which would benefit from revised implementations and more current checks. A revised set of baseline configurations that would benefit NCCS’s systems deployment and maintenance infrastructure were identified. Considering that NCCS primarily uses a “Puppet” cloning configuration management tool in deploying its system stacks, a crucial step in the process is determining the representative node, the most compliant system, considering the cloning method used, that is used in the cloning of the rest of the service stack. Despite the “puppet” cloning method being commonly used by the NCCS, there are still other cloning approaches that are used, hence why this security evaluation was done comprehensively to allow the consideration of multiple systems deployment techniques currently in use by the NCCS. The study proved to be very successful in assessing the revision of NCCS’s security standards, baselines, and implementations and the overall improvement of NCCS’s security posture and missions and systems operations.


Scaptest1: Number of Checks (Reported Severity)
■ High
■ Medium
■ Low
■ Unknown


Scaptest1: Number of Checks (Determined Severity)
■ High
■ Medium
■ Low
■ Low-High