U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

Near Term Vulnerability Mitigation

OAK RIDGE National Laboratory

Real-time threat validation for secure, actionable information sharing for cyber response

The project team provides a capability for vulnerability validation to be rapidly conducted in order to address challenges and provide vendors with secure, authenticated, information sharing via discreet methods for their use and for corrective action. This communication mechanism relays information while simultaneously validating malware and device/system vulnerabilities. This solution lowers the cybersecurity risk for vendors and utilities while sharing malware or vulnerability information.

KEY TAKEAWAYS

- Removes the isolation of cyber targets that rely on their own expertise and existing relationships with vendors, suppliers, and similar companies to address and mitigate risk
- Develops a rapid response mechanism for specific, targeted cyberattacks or vulnerabilities
- Provides unbiased validation of vulnerabilities

OUTCOME

This project develops and delivers an operational methodology for rapid vulnerability validation with the relaying of cyber vulnerabilities directly to vendors and end-users. The team delivers a communications map for operational technology vulnerabilities, including a reporting structure and cybersecurity plan for data handling and storage. Coordinated scientifically based and executed vulnerability validation testing at Oak Ridge National Laboratory incorporates methods of evaluation of relevant attempted attacks from the field, which will help determine whether the attacker could exploit a real vulnerability.

PARTICIPANTS	ROLE
OAK RIDGE National Laboratory	Project lead; coordinates the establishment of a secure communications mechanism with third parties to disclose vulnerability test results with a focus on legacy equipment.
EMERSON	Validates the efficacy of the developed information communication mechanism.
Schneider Electric	Provides vendor-centric review of vulnerability communication of vulnerabilities from discovery to mitigation.
ExxonMobil	Oil and gas end-user; expert in cybersecurity vulnerability information sharing.
DUKE ENERGY	Integrated electric utility end user; expert in cybersecurity vulnerability information sharing.
epb	Distribution electric utility; performance utilization verification of project's information sharing product

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Peter Fuhr
Project Manager, Principal Investigator
Oak Ridge National Laboratory
865-574-8529
fuhrpl@ornl.gov

Current Contact as of February 2020:

Akhlesh Kaushiva
Senior Technical Systems and Cybersecurity Advisor
Department of Energy (DOE)
Office of Cybersecurity, Energy Security, and Emergency Response (CESER)
202-287-6062
Akhlesh.Kaushiva@hq.doe.gov

Period of Performance: July 2018 – July 2019

Total Award Value: $499,678
DOE Share: $499,678
Cost Share: $0

CYBERSECURITY FOR ENERGY DELIVERY SYSTEMS (CEDS)

CEDS projects are funded through DOE CESER, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyberattacks.

Website: https://www.energy.gov/ceser

Date Written: June 2021