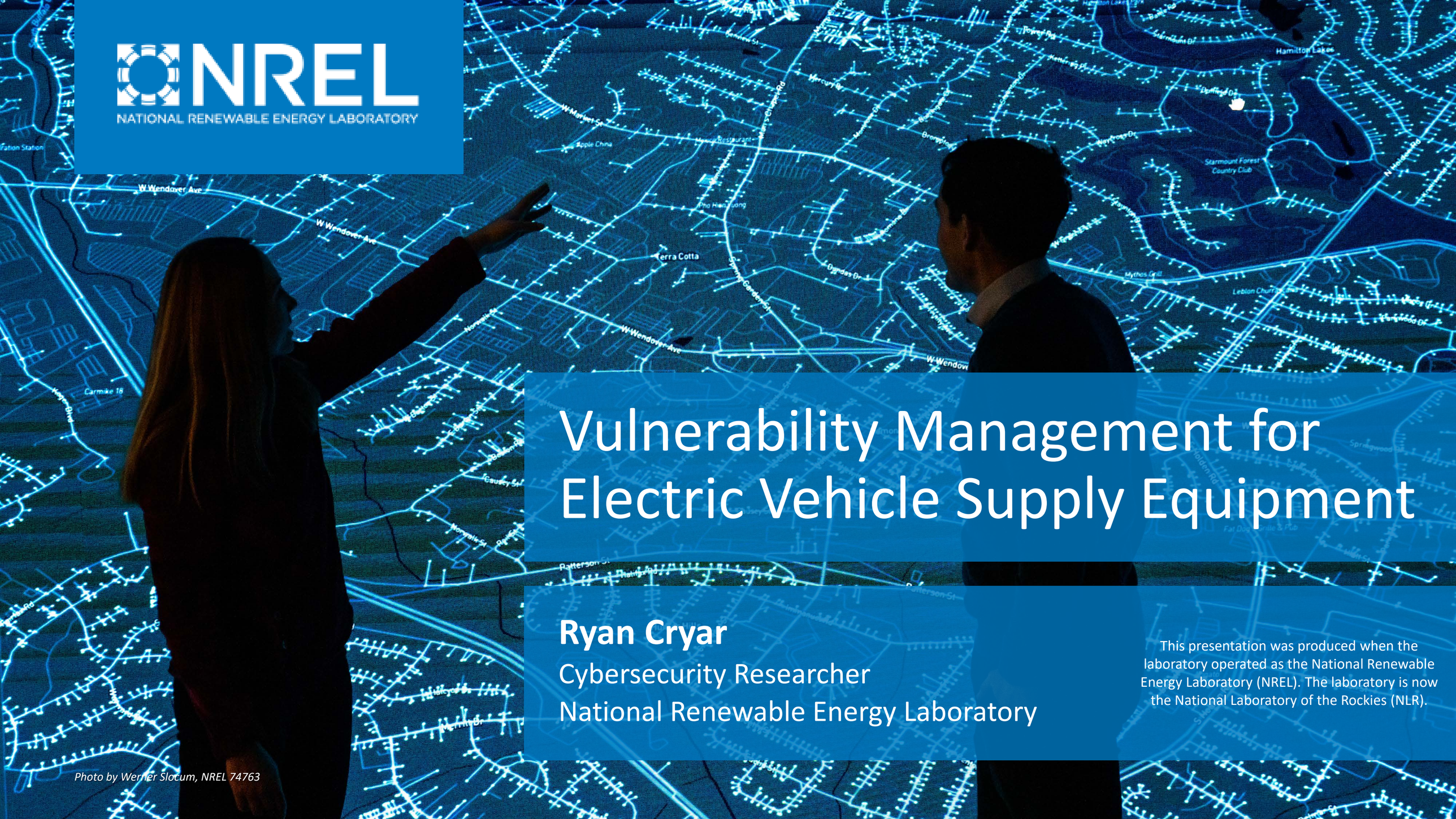


Vulnerability Management for Electric Vehicle Supply Equipment

Ryan Cryar
Cybersecurity Researcher
National Renewable Energy Laboratory

This presentation was produced when the laboratory operated as the National Renewable Energy Laboratory (NREL). The laboratory is now the National Laboratory of the Rockies (NLR).

Photo by Werner Slocum, NREL 74763

Purpose

- Managing vulnerabilities across multiple stakeholders within electric vehicle charging infrastructure (EVCI) can be a large undertaking.
- The interconnected nature of these systems exposes them to a wide range of cybersecurity risks.
- This requires a holistic approach to address vulnerabilities across the EVSE components.

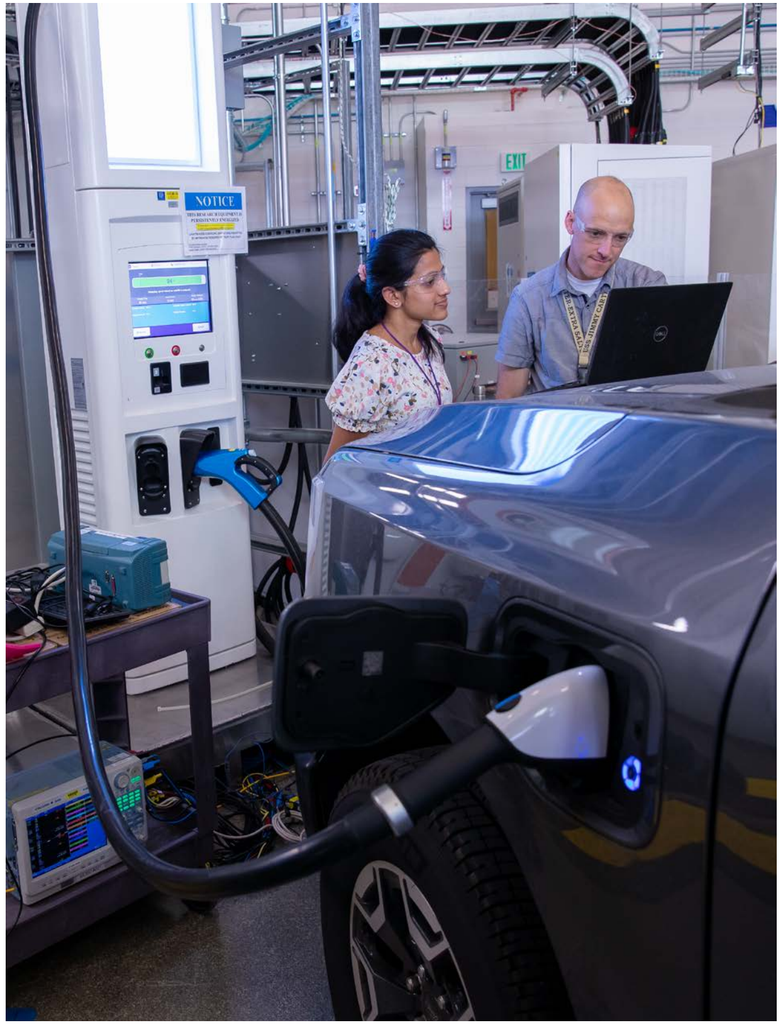
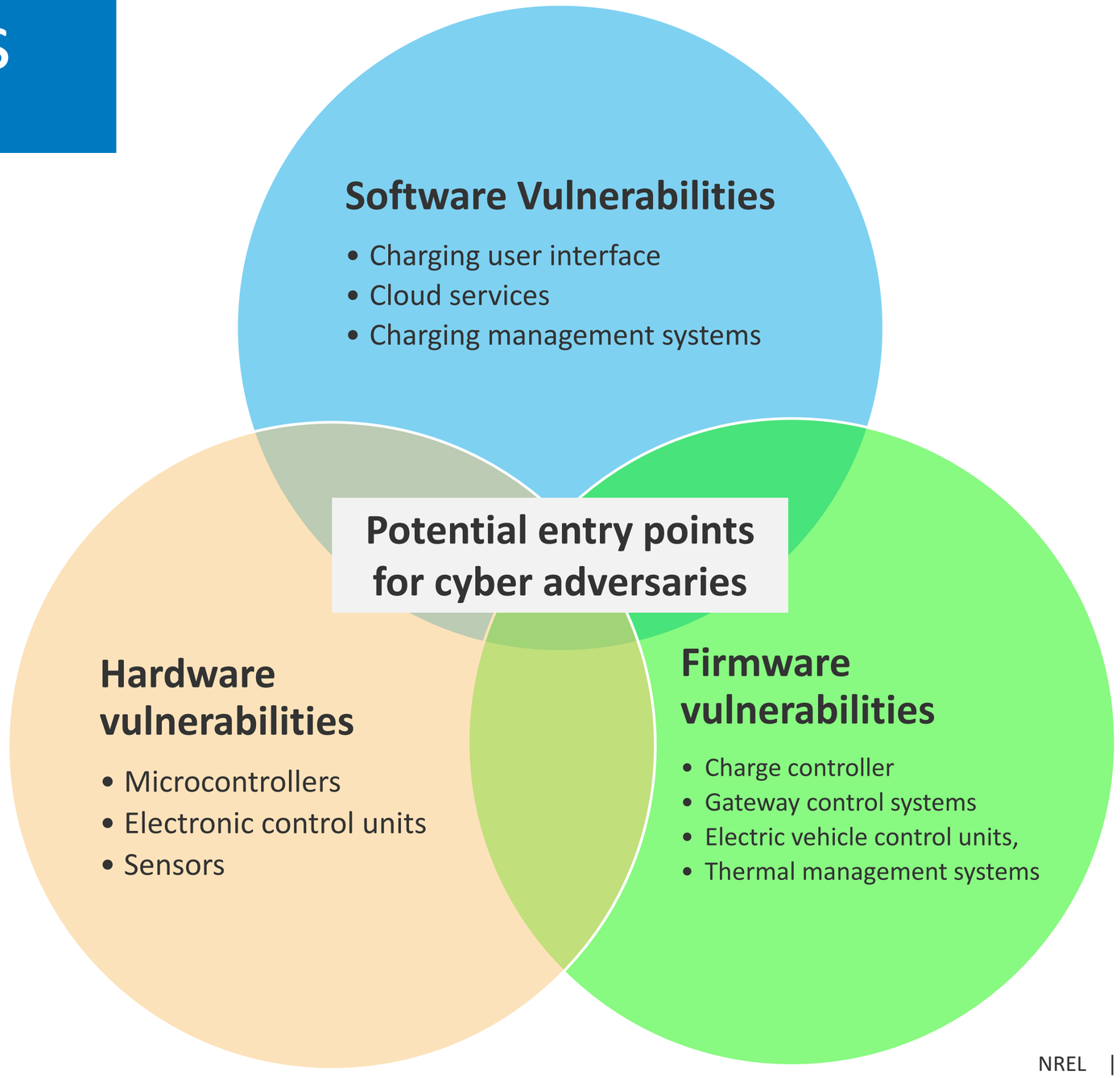


Photo by Joe DelNero, NREL 82750

Vulnerability Layers

- Vulnerabilities are not just in software.
- A diverse stakeholder group and set of technologies make vulnerability management a large undertaking.
- A strongly skilled workforce is required to ensure vulnerabilities are managed across all technologies.



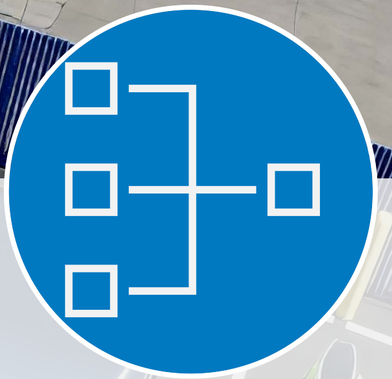
Impacted Stakeholders

Vehicle Original Equipment Manufacturers

Utilities

Third-Party Vendors

Consumers



Charge Network Operators

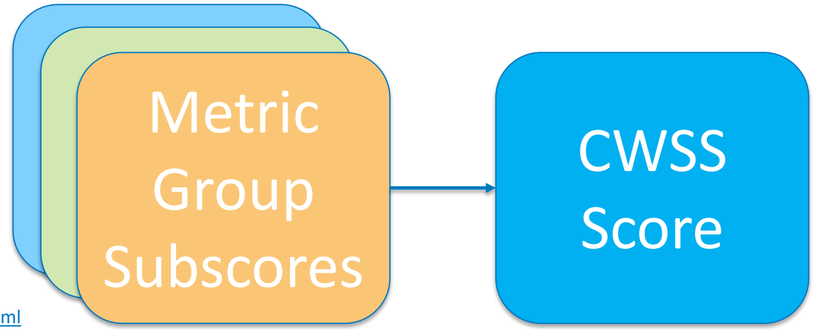
Photo by NACFE's Run on Less – Electric DEPOT

Responsible Parties

Team	Responsibilities
Cybersecurity Teams	Threat detection, incident response, vulnerability coordination
Software Engineering Teams	Ensuring vulnerabilities are patched, coordination with cyber team, conducting over the air updates, ensuring secure development practices, cyber-informed engineering
Operations Teams	Coordination required to ensure all identified assets are updated within an appropriate timeframe according to the severity of the vulnerability, conducting cybersecurity training
Utilities	Coordination with suppliers to ensure all systems are up to date, preliminary testing before deployment

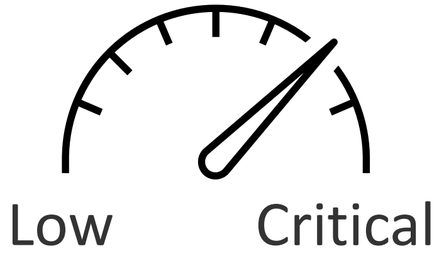
Vulnerability vs. Weakness

- A Common Weakness Enumeration (CWE) is a weakness that becomes a vulnerability.
- A CWE is the root mistake in the code.
- The intensity of the CWE is scored via the Common Weakness Scoring System (CWSS).



Source: https://cwe.mitre.org/cwss/cwss_v1.0.1.html

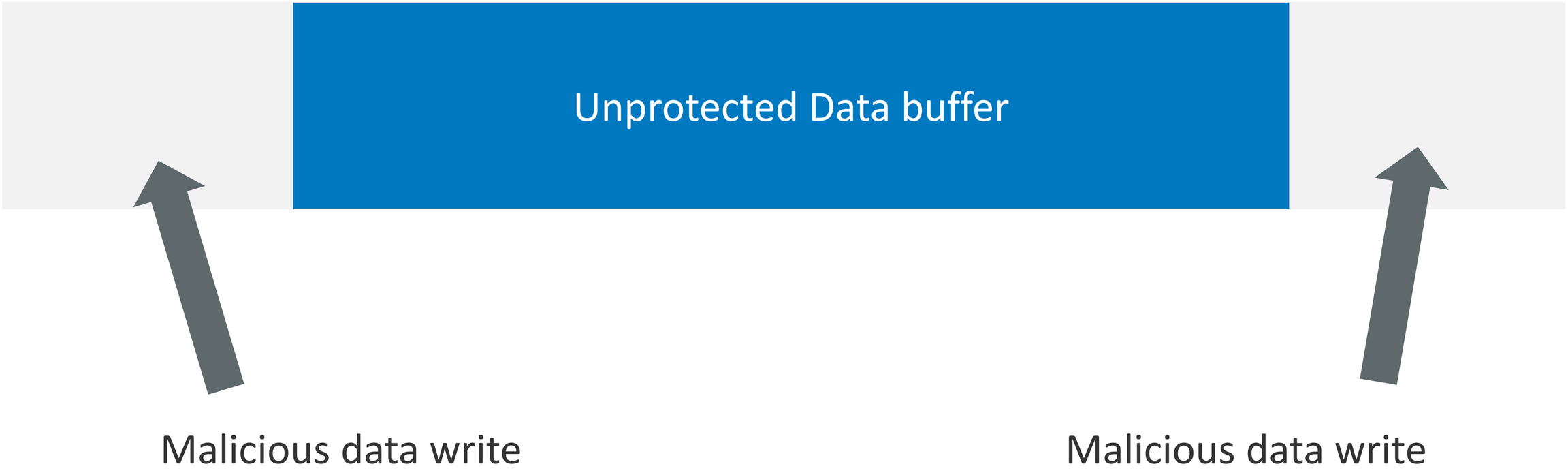
- Common Vulnerabilities and Exposures (CVE) are vulnerabilities stemming from a CWE that is specific to a product.
- The CVE tracks the vulnerability caused by said mistake.
- CVEs are scored through Common Vulnerability Scoring System (CVSS).



Weakness Example: Out of Bounds Write

CWE-787 Out of bounds write: Data is written past the end or before the beginning of the intended buffer.

Memory

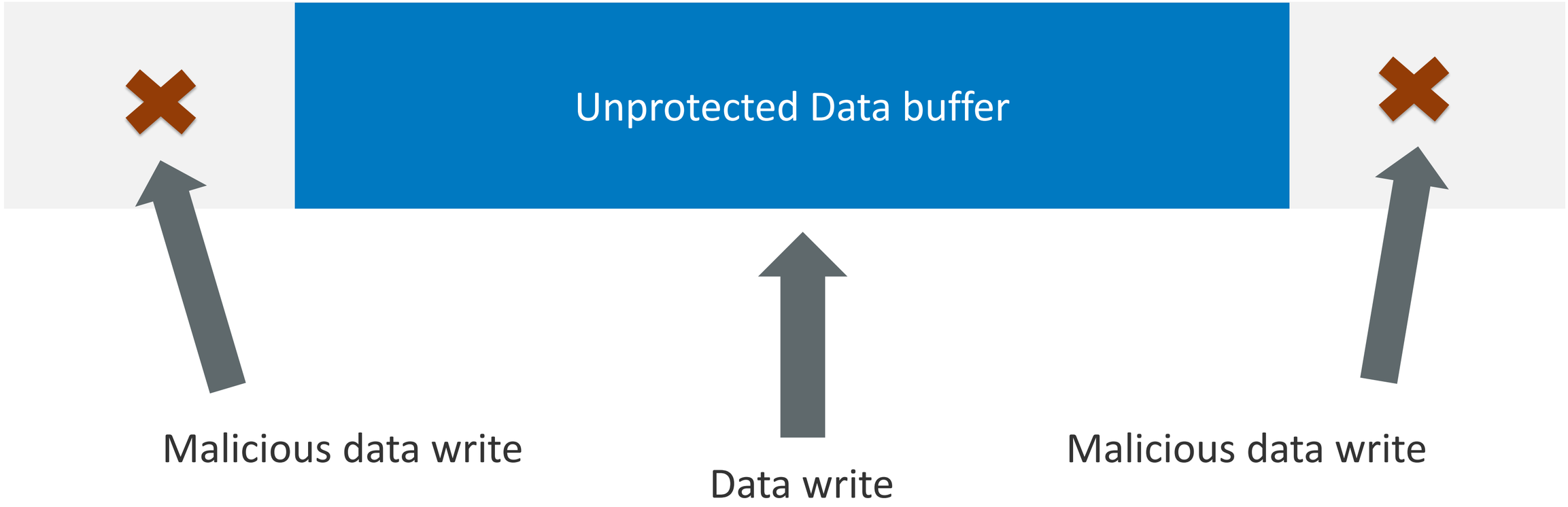


Source: https://cwe.mitre.org/data/definitions/787.html

Weakness Example Patch

CWE-787 Out of bounds write

Memory



Source: https://cwe.mitre.org/data/definitions/787.html

Vulnerability Through Weakness

- **CVE-2021-28664**: Privilege escalation in Arm Mali GPU Driver
  - Utilizing CWE-787: Out of bounds write, an unprivileged user can achieve read/write access to read only pages
  - Exploited in the wild per CISA's Known Exploited Vulnerabilities catalog
  - Users instructed to conduct upgrades as soon as possible
  - Conducting upgrades is easier said than done

Source: https://nvd.nist.gov/vuln/detail/CVE-2021-28664

Coordinated Vulnerability Disclosure (CVD)

In a multi-stakeholder industry, it is critical to ensure vulnerability information is shared and acted on.

Photo by Josh Bauer, NREL 90594

- CVD relies on security researchers to report vulnerabilities found in software or hardware to vendors.
- The vendors then patch and deploy the fix before the vulnerability is publicly disclosed for the sake of information sharing.

Roles in Coordinated Vulnerability Disclosure (CVD)

Conducting effective CVD requires several key roles in an organization.

Role	Description
Reporter/Finder	Often external to the organization. The discoverer of a vulnerability who then reports it to the vendor.
Vendor	The organization who receives the vulnerability from the finder and is responsible for patching the vulnerability.
Coordinator	The entity that is the information broker between stakeholders.
Deployer	The entity that deploys the product with the vulnerability.

Source: https://certcc.github.io/CERT-Guide-to-CVD/topics/roles/vendor/

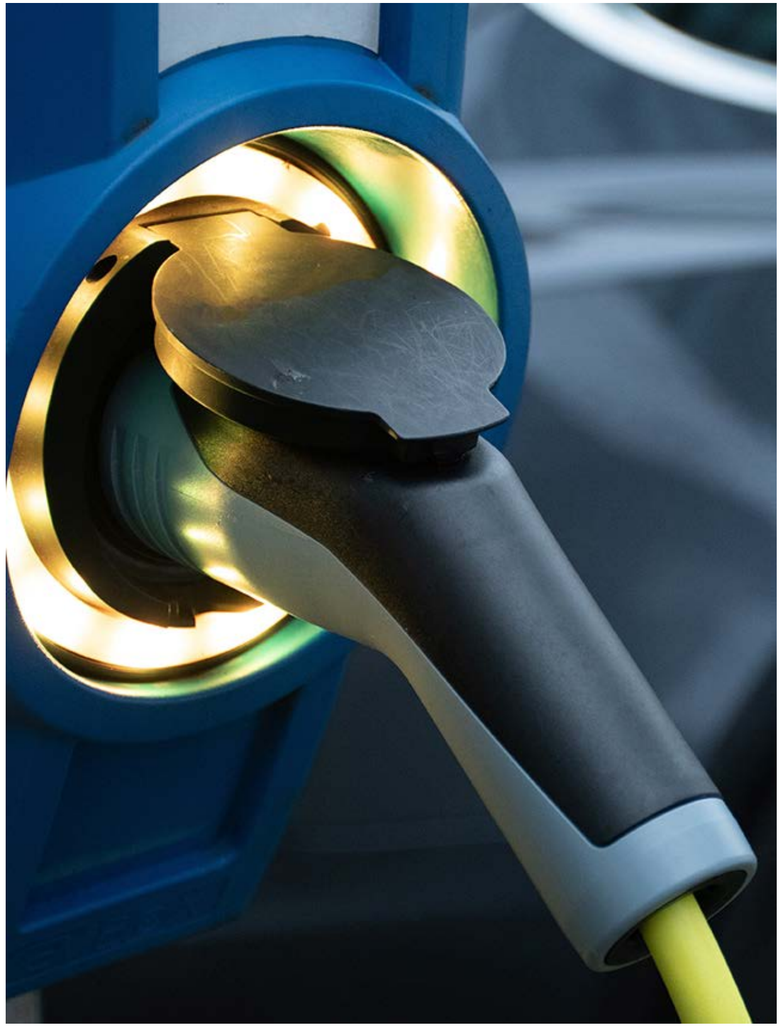
CVD Challenges

- Sharing information and ingesting vulnerabilities through CVD relies on a cyber mature vendor
- Ingesting found vulnerabilities can be challenging for smaller organizations that do not have dedicated cyber teams
- Prioritizing vulnerabilities reported within a patch cycle
- Deploying patch that can still maintain interoperability across all customers
- Identifying and implementing best practices
- Lacking specific workforce development and training

Source: https://certcc.github.io/CERT-Guide-to-CVD/topics/roles/vendor/

Unique Challenges for EVCI

- Protocols are unique and quite challenging to understand
- Some systems may not be able to be updated depending on their interoperability with other components
- Many stakeholders in the distributed ecosystem
- Many endpoint devices and connected infrastructure
- Maintaining supply chain tractability
- Testing and validation of equipment is a large undertaking
- A lacking stakeholder-specific training on cybersecurity



Source: https://certcc.github.io/CERT-Guide-to-CVD/topics/roles/vendor/

Common Resources

- Software Engineering Institute Computer Emergency Response Team (CERT) Coordination Center
  - Guide to Coordinated Vulnerability Disclosure
  - Vulnerability Information and Coordination Environment (VINCE) platform
- Vulnerability management systems such as Tenable or Qualys
- Security unit testing through the Open Worldwide Application Security Project (OWASP) Top 10
- NIST Cybersecurity Framework
- CISA Risk and Vulnerability Assessments mappings
- Red Canary Atomic Red Team test library

Coming Soon: Blueprint for Coordinated Vulnerability Disclosure

- The idea is to “jump start” what is needed to set up a CVD program with a **blueprint tool that details step-by-step processes**.
- This leads to capabilities to participate in more mature programs such as an Information Sharing and Analysis Center or a bug bounty program.
- The end goal is enabling organizations to “self mature” through:
    - Applying the blueprint to their own organizational practices
    - Learning secure coding practices
    - Coordinating stakeholder critical specific information safely and securely.

Thank You!

Ryan.Cryar@nrel.gov

NLR/PR-5T00-94504

This work was authored by NREL for the U.S. Department of Energy (DOE), operated under Contract No. DE-AC36-08GO28308. Funding provided by the U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Vehicle Technology Office. The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.