CWE ICS/OT Special Interest Group

- Mission and Initial Guidance -

In partnership with the U.S. Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER), the CWE program – operated by the CISA-funded Homeland Security Systems Engineering and Development Institute (HSSEDI) – launched a special interest group (SIG) focusing on security weaknesses in industrial control systems (ICS) and operational technology (OT): the CWE ICS/OT SIG.

Background
The CWE ICS/OT SIG offers a forum for researchers and technical representatives from organizations operating in ICS/OT design, manufacturing, and security to interact, share opinions and expertise, and leverage each other's experiences in supporting continued growth and adoption of CWE as a common language for defining ICS/OT security weaknesses. Participants include ICS/OT vulnerability researchers, engineers, security professionals, and companies representing OEMs/system integrators, tools/infrastructure vendors, and asset owners and operators. Managers and other organizational leaders are also welcome, although it is preferred that they are accompanied by technical staff.

Objective
While IT has an extant body of work related to identify and classifying security weaknesses, IT and ICS/OT are different, and existing IT classifications are not always useful in describing and managing security weaknesses in ICS/OT systems. Addressing this gap will help all stakeholders communicate more efficiently and effectively and promote a unity of effort in identifying and mitigating ICS/OT security weaknesses, especially in critical infrastructure.

Accomplishments
As a result of the CWE ICS/OT SIG, CWE version 4.7 added a new collection of weaknesses relevant to ICS/OT broken down by the Securing Energy Infrastructure Executive Task Force (SEI ETF)'s 20 Categories of Security Vulnerabilities for ICS, including ICS Communications, Dependencies and Architecture, Supply Chain, Engineering (Constructions/Deployment), Operations, and Maintenance. This new CWE-View includes 81 weaknesses across 26 categories.

The CWE ICS/OT SIG also published mappings between the ISA/IEC 62443 set of standards and the CWE corpus. These mappings can be seen here: https://cwe.mitre.org/data/definitions/1424.html Additional information can be found in the following repository: https://github.com/CWE-CAPEC/ICS-OT_WorkingGroup

As of Summer 2023, the ICS/OT SIG does not meet on a regular basis. When feasible, the SIG does meet on an ad-hoc basis to collaborate and evolve CWE ICS/OT information for additional value to the stakeholder community. There are currently no plans to establish a recurring meeting cadence.

For more information, and to be added to the CWE ICS/OT SIG emailing list, please email cwe@mitre.org