Panel: Coordinating vulnerabilities in AI systems

Harold Booth (NIST)

Jonathan Evans (MITRE)

Ian Malloy (IBM)

Lena Pons (Carnegie Mellon University)

Moderator: Jonathan Spring

Thanks to Brian Lindauer, Zach Kurtz, and Frank Stein for their help organizing this panel

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM19-1174

Vulnerability management basics

Vulnerability

- a weakness in an information system, including in its system security procedures, internal controls, requirements, design, or implementation, that could be exploited or triggered by a threat source. (NIST docs define each of these words in turn)

Vulnerability management includes (per FIRST):

- Vulnerability discovery / research
- Vulnerability report intake
- Vulnerability analysis
- Vulnerability coordination
- Vulnerability disclosure
- Vulnerability response

Vulnerability management basics II

CVSS

- "The Common Vulnerability Scoring System provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its [technical] severity." (FIRST, https://www.first.org/education/csirt_services_framework_v2.0)

NIST's National Vulnerability Database (NVD) "performs analysis on CVEs that have been published to the CVE Dictionary. NVD staff are tasked with analysis of CVEs… . This analysis results in association impact metrics (Common Vulnerability Scoring System - CVSS), vulnerability types (Common Weakness Enumeration - CWE), and applicability statements (Common Platform Enumeration - CPE)…" https://nvd.nist.gov/general

Panelists

Harold Booth

Jonathan Evans

Ian Malloy

Lena Pons