Navigating the Patchwork: Investigating the Availability & Consistency of Security Advisories

Ronald Thompson, Luke Boshar, Eugene Y. Vasserman, and Daniel Votipka

Tufts University

Kansas State University

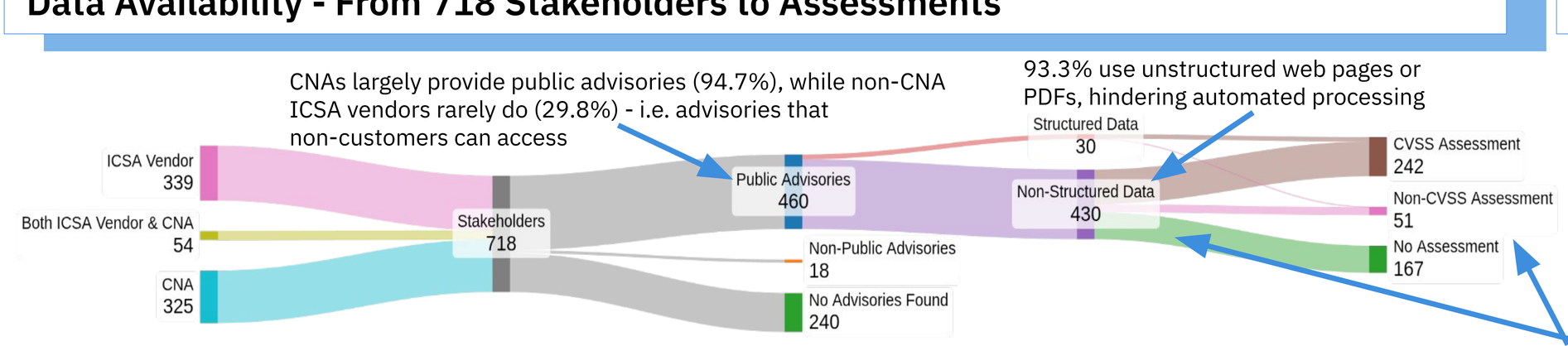
Motivation

- Effectively prioritizing patches requires **accessible and consistent vulnerability information**, but the current ecosystem presents significant challenges.
- System administrators must triage vulnerabilities based on severity, but they struggle to find comprehensive information from the **patchwork of disparate public advisories**.
- While prior work highlights specific issues, a **broader, empirical baseline characterization** of the advisory ecosystem has been lacking.
- Stakeholders selected from CVE Naming Authorities (CNAs) and vendors mentioned in CISA's Industrial Control Systems Advisories (ICSAs) - who are governed by vulnerability disclosure requirements

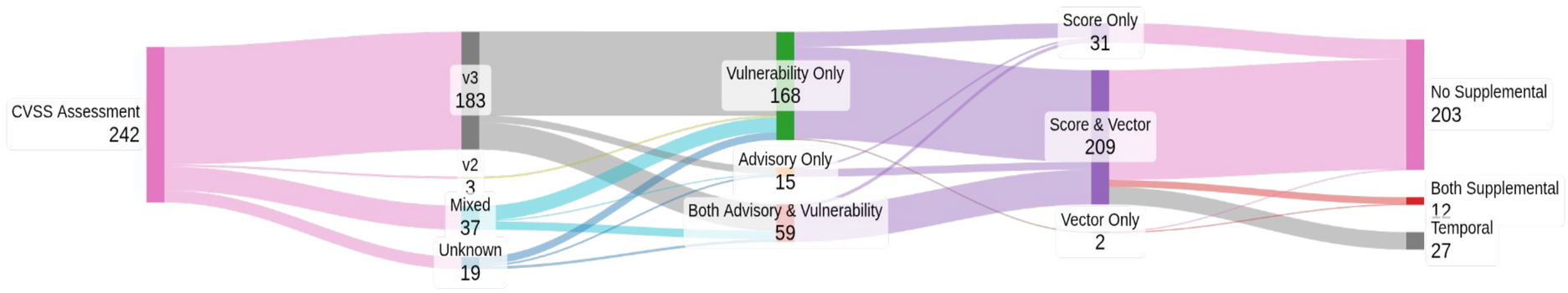
Research Questions

- How available and accessible are security advisories, i.e. notices that contain vulnerability information?
- How often are these presented in a structured, easily machine-processable format?
- How consistently do advisories report Common Vulnerability Scoring System (CVSS) information for vulnerabilities in their advisories?

Data Availability - From 718 Stakeholders to Assessments



Data Consistency - A Breakdown of 242 CVSS Assessments



Takeaways

CONSIDERABLE FRICTION IN THE PUBLIC ADVISORY ECOSYSTEM, making it difficult for operators and researchers to collect and compare information at scale.

Lack of structured data and transparent, consistent CVSS reporting forces security teams into **MANUAL TIME-CONSUMING ANALYSIS**, delaying crucial patching decisions.

Critical need for **ACTIVE COORDINATION AUTHORITIES** and improved standards to help stakeholders enhance reporting consistency and transparency

U.S. AIR FORCE NSF Medcrypt