CVE Lightning Talk 2022

The CVE Program

The CVE Program's mission is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

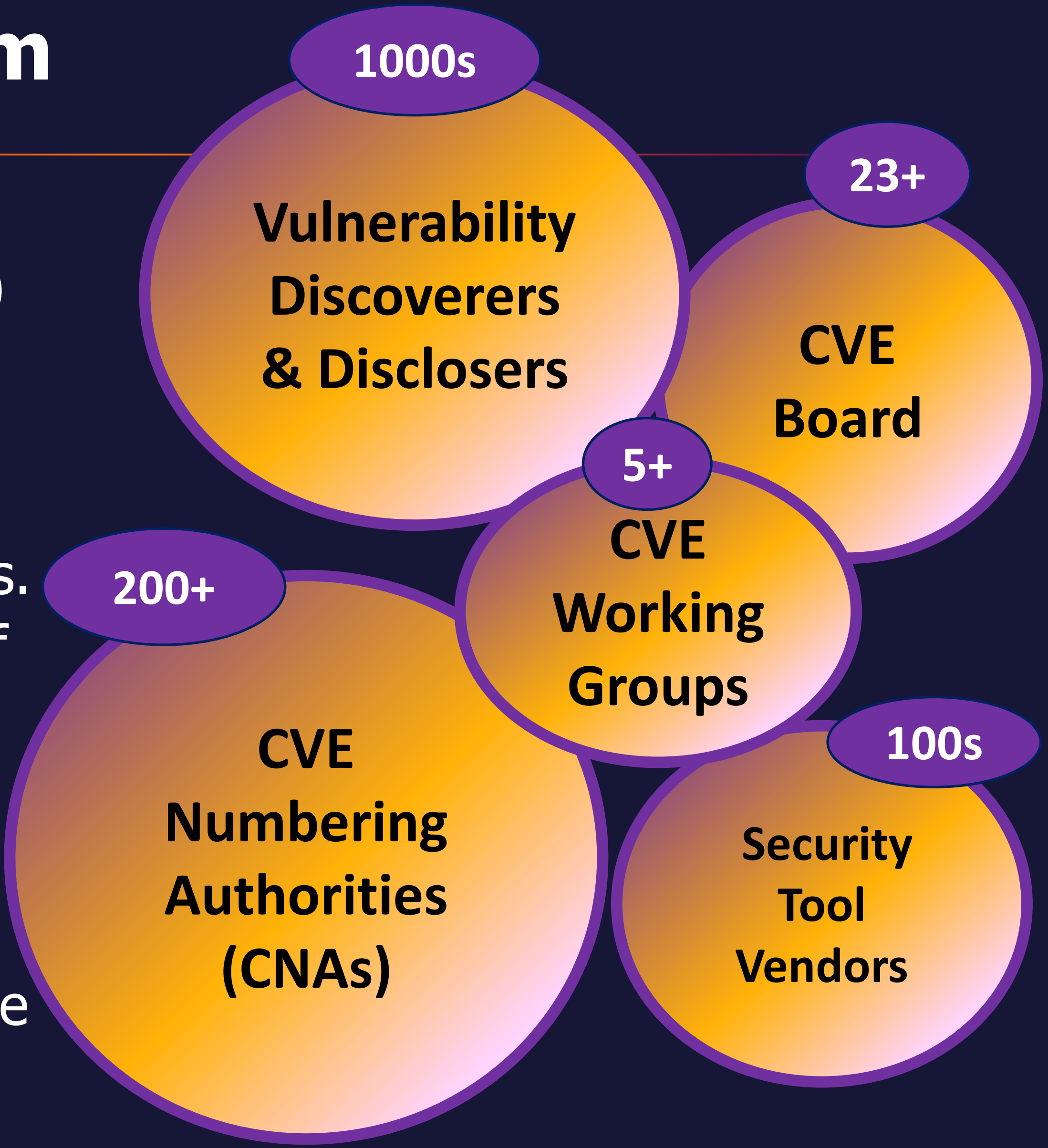
CVE is an international, community-based effort and relies on the community to discover vulnerabilities. The vulnerabilities are discovered, then assigned a CVE ID, and published to the CVE List.

CVE enables two or more people or tools to refer to a vulnerability and know they are talking about the same thing, resulting in significant time and cost savings.

All photos on this slides: is by Unknown Author is licensed under CC BY-NC

A Community Driven Program

- The CVE Program relies on the community (vendors, end users, researchers, and more) to discover and register vulnerabilities.
- CVE IDs are assigned by CVE Numbering Authorities (CNAs), which are operated on a voluntary basis by participating organizations.
- The CVE Board, which drives the direction of the CVE Program, consists of industry, academic, and government representatives from around the world.
- CVE Working Groups develop the program's policies (approved by the CVE Board) and are open to the community.



1000s
Vulnerability Discoverers & Disclosers

23+
CVE Board

5+
CVE Working Groups

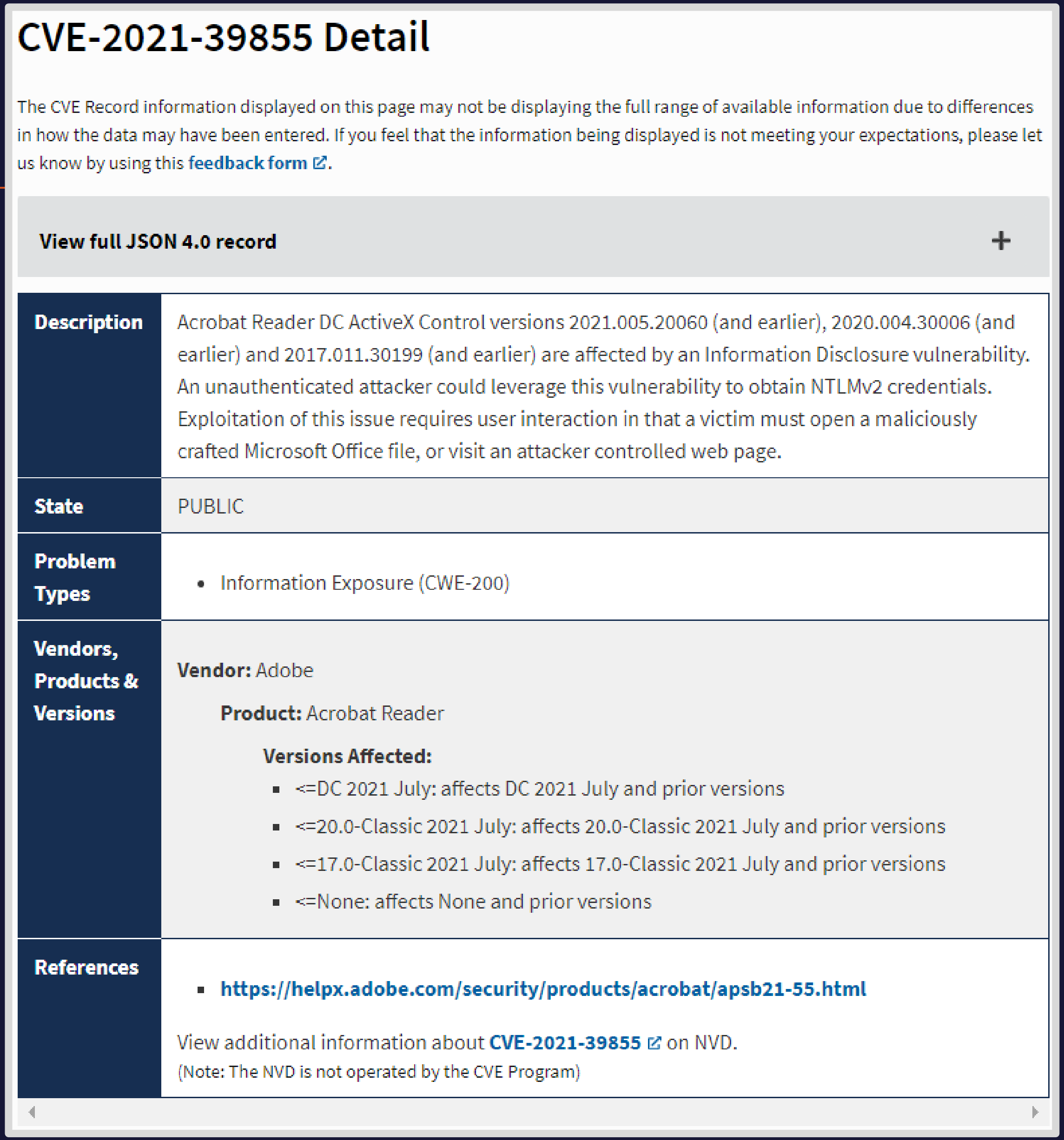
200+
CVE Numbering Authorities (CNAs)

100s
Security Tool Vendors

What is a CVE?

- **A CVE Record** is the descriptive data about a Vulnerability associated with a CVE ID, provided by a CNA. This data is provided in multiple human and machine-readable formats.

This is a CVE Record



CVE-2021-39855 Detail

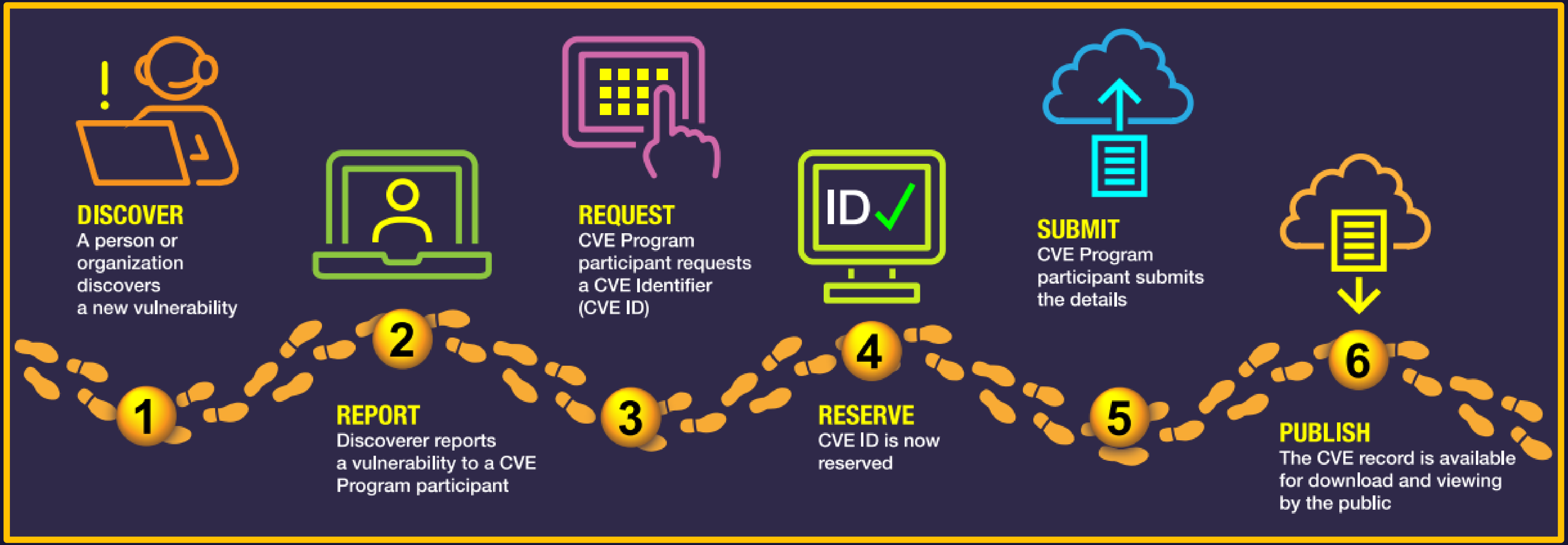
The CVE Record information displayed on this page may not be displaying the full range of available information due to differences in how the data may have been entered. If you feel that the information being displayed is not meeting your expectations, please let us know by using this feedback form.

View full JSON 4.0 record +

Description	Acrobat Reader DC ActiveX Control versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by an Information Disclosure vulnerability. An unauthenticated attacker could leverage this vulnerability to obtain NTLMv2 credentials. Exploitation of this issue requires user interaction in that a victim must open a maliciously crafted Microsoft Office file, or visit an attacker controlled web page.
State	PUBLIC
Problem Types	• Information Exposure (CWE-200)
Vendors, Products & Versions	**Vendor:** Adobe **Product:** Acrobat Reader **Versions Affected:** ▪ <=DC 2021 July: affects DC 2021 July and prior versions ▪ <=20.0-Classic 2021 July: affects 20.0-Classic 2021 July and prior versions ▪ <=17.0-Classic 2021 July: affects 17.0-Classic 2021 July and prior versions ▪ <=None: affects None and prior versions
References	• https://helpx.adobe.com/security/products/acrobat/apsb21-55.html View additional information about CVE-2021-39855 on NVD. (Note: The NVD is not operated by the CVE Program)

How does it work?

- **CVE Record Lifecycle**



1 **DISCOVER**
A person or organization discovers a new vulnerability

2 **REPORT**
Discoverer reports a vulnerability to a CVE Program participant

3 **REQUEST**
CVE Program participant requests a CVE Identifier (CVE ID)

4 **RESERVE**
CVE ID is now reserved

5 **SUBMIT**
CVE Program participant submits the details

6 **PUBLISH**
The CVE record is available for download and viewing by the public

CVE®

CVE Numbering Authority

- **What is a CNA?**
  - An organization responsible for the regular assignment of CVE IDs to vulnerabilities, and for creating and publishing information about the vulnerability in the associated CVE Record. Each CNA has a specific Scope of responsibility for vulnerability identification and publishing.
- **A CNA may be a:**
  - Software vendor
  - Open-source project
  - Coordination Center
  - Bug Bounty service provider
  - Vulnerability Researcher(s)
  - Hosted Service

Why become a CNA?

- Demonstrate mature vulnerability management practices and a commitment to cybersecurity to current and potential customers.
- Communicate value-added vulnerability information to your customer base.
- Control the CVE publication release process for vulnerabilities in your scope.
- Assign CVE IDs without having to share embargoed information with another CNA.
- Share your information to protect systems against attacks globally.
- Join the CVE community and exchange ideas with other CNA organizations.

Requirements for becoming a CNA

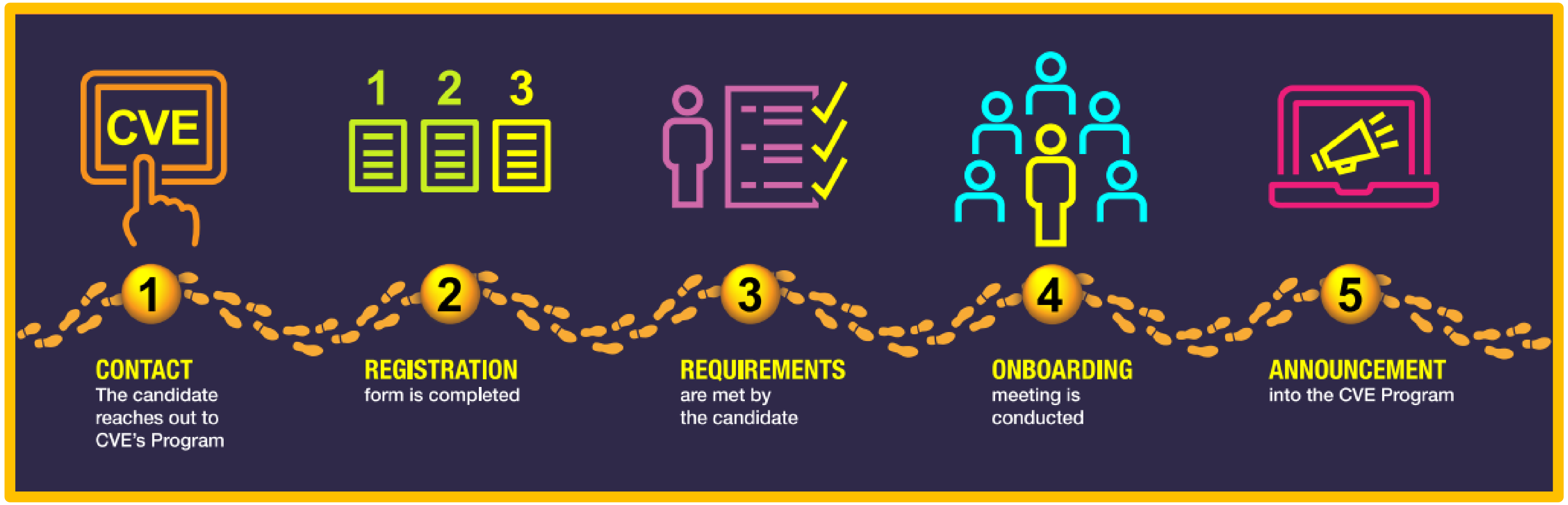
- Have a public vulnerability disclosure policy.
- Have a public source for new vulnerability disclosures.
- Agree to the CVE Terms of Use.

This Photo by Unknown Author is licensed under CC BY-SA

Cost of being a CNA

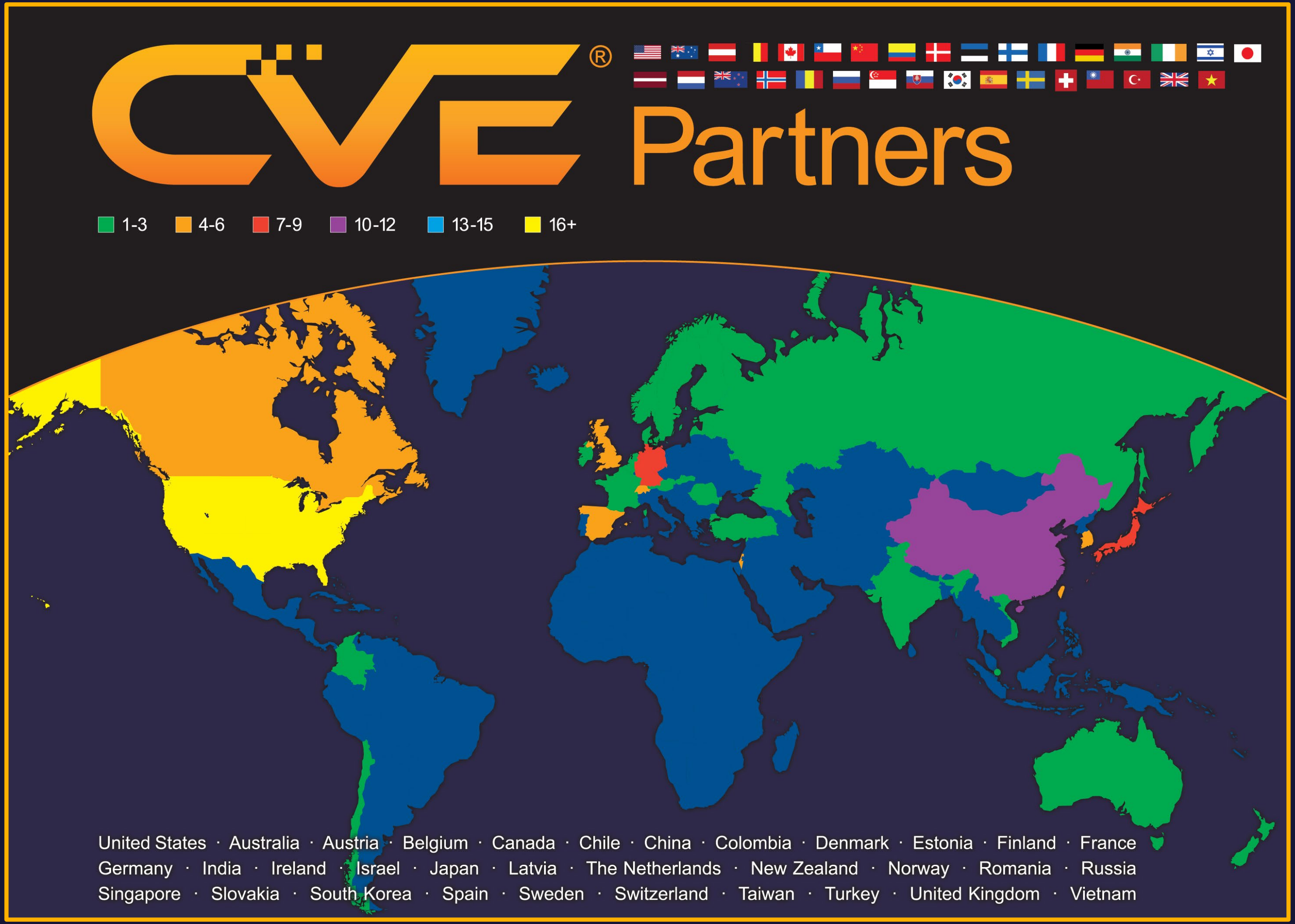
- There is no monetary fee.
- There is no contract to sign.
- CNAs volunteer their own time for their own benefit.

How to become a CNA



1. Contact the CVE Program
2. Complete the registration form
3. Agree to the CVE Terms of Use
4. Attend the introductory session
5. Successfully complete practice examples

212 Partners in 33 countries



United States · Australia · Austria · Belgium · Canada · Chile · China · Colombia · Denmark · Estonia · Finland · France
Germany · India · Ireland · Israel · Japan · Latvia · The Netherlands · New Zealand · Norway · Romania · Russia
Singapore · Slovakia · South Korea · Spain · Sweden · Switzerland · Taiwan · Turkey · United Kingdom · Vietnam

The mission of the CVE Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

There is one CVE Record for each vulnerability in the catalog. The vulnerabilities are discovered then assigned and published by organizations from around the world that have partnered with the CVE Program. Partners publish CVE Records to communicate consistent descriptions of vulnerabilities. Information technology and cybersecurity professionals use CVE Records to ensure they are discussing the same issue, and to coordinate their efforts to prioritize and address the vulnerabilities.

Learn more www.cve.org

CVE is sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA).