Common Vulnerabilities and Exposures

Common Vulnerabilities and Exposures and the CNA Program

15 May 2017

Daniel Adinolfi, The MITRE Corporation
@pkdan14850

Contents

- **CVE Overview**
- **CVE Numbering Authority (CNA) Program**
  - The CNA role
  - Benefits of participating as a CNA
- **CNA Program Administrative Structure**
  - Federated and adapting framework
- **Participation in the CNA Program**

CVE Overview

CVE Description, Purpose, and Value

- CVE is a dictionary of publicly known cybersecurity vulnerabilities

- Purpose: To uniquely identify and name publicly disclosed vulnerabilities pertaining to specific versions of software or codebases

- Value: Stakeholders have confidence that they can refer to a CVE Identifier (ID) and know they are talking about a specific, unique vulnerability regardless of the tool or forum being used

What CVE Is and Is Not

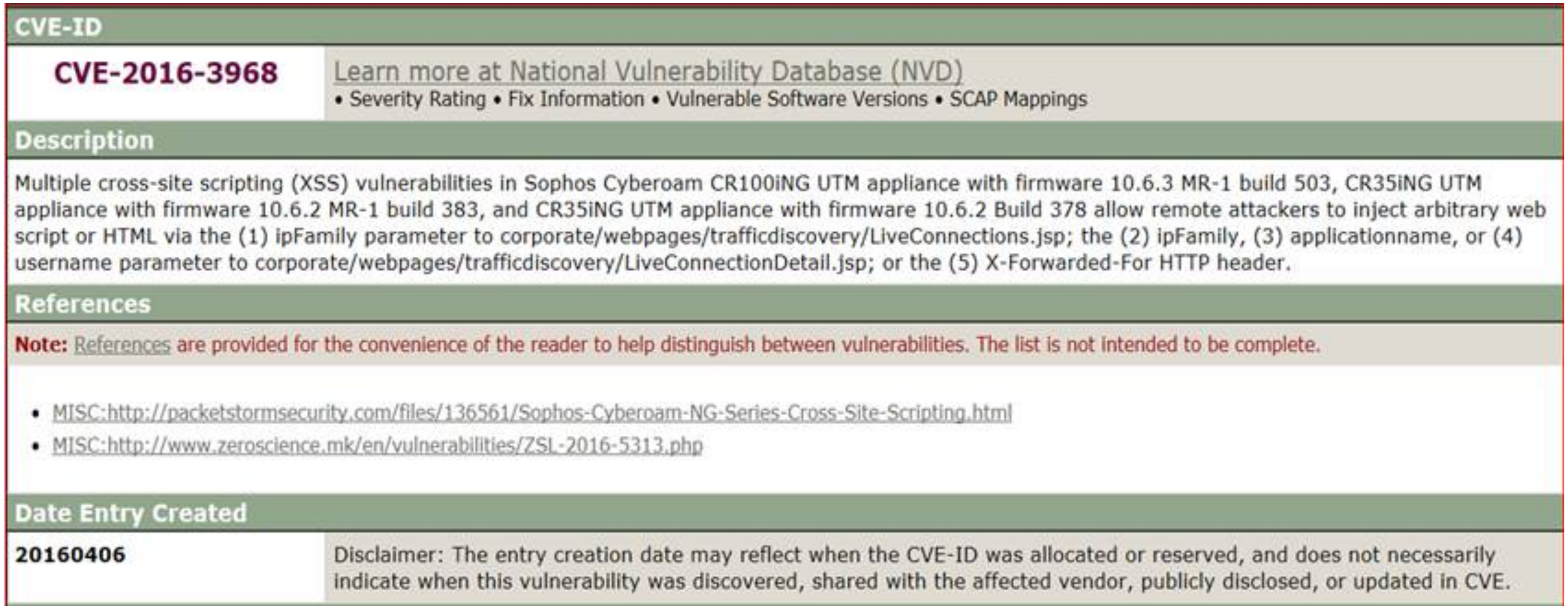
CVE is…

- **The de facto standard for uniquely identifying vulnerabilities**
- **A dictionary of publicly known cybersecurity vulnerabilities**
- **A pivot point between vulnerability scanners, vendor patch information, patch managers, and network/cyber operations**

CVE is not…

- **A vulnerability mitigation**
  - CVE IDs uniquely define vulnerabilities so that mitigations can be efficiently applied
- **A vulnerability database**
  - CVE allows vulnerability databases to be linked together under commonly used IDs
- **A source for vulnerability risk, impact, fix, or technical information**
  - Each CVE contains a unique ID, description, and references
- **A tool for publicly disclosing vulnerabilities**
  - CVE uses publicly disclosed vulnerability information as its source of information

CVE Example



CVE-ID

CVE-2016-3968

Learn more at National Vulnerability Database (NVD)

• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

Multiple cross-site scripting (XSS) vulnerabilities in Sophos Cyberoam CR100iNG UTM appliance with firmware 10.6.3 MR-1 build 503, CR35iNG UTM appliance with firmware 10.6.2 MR-1 build 383, and CR35iNG UTM appliance with firmware 10.6.2 Build 378 allow remote attackers to inject arbitrary web script or HTML via the (1) ipFamily parameter to corporate/webpages/trafficdiscovery/LiveConnections.jsp; the (2) ipFamily, (3) applicationname, or (4) username parameter to corporate/webpages/trafficdiscovery/LiveConnectionDetail.jsp; or the (5) X-Forwarded-For HTTP header.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:http://packetstormsecurity.com/files/136561/Sophos-Cyberoam-NG-Series-Cross-Site-Scripting.html
- MISC:http://www.zeroscience.mk/en/vulnerabilities/ZSL-2016-5313.php

Date Entry Created

20160406

Disclaimer: The entry creation date may reflect when the CVE-ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

CVE Numbering Authority (CNA) Program

CVE Numbering Authorities (CNAs)

- CNAs are organizations that assign CVE IDs to researchers and vendors for inclusion in first-time public announcements of new vulnerabilities
- CNAs participate in the CVE Program in accordance with CNA Rules
- Each CNA has a specific scope of responsibility, delimiting what products, information sources, or domains for which they assign CVEs

Benefits of Participating as a CNA

- **The ability to publicly disclose new vulnerabilities with CVE IDs assigned to them at the time of disclosure without having to wait for the CVE ID assignment to be done by another entity**
- **Direct notification of vulnerabilities in the organization's products by researchers who must request a CVE ID from them**
- **The ability to better control their own vulnerability disclosure process**
  - Per company policy and practice
  - Per national policy and practice

The CNA Program Administrative Structure

Federated CVE

The Vision

A global, federated system of vulnerability identifiers evolved from today's CVE, with a defined common naming convention and an *active and engaged* set of collaborating community and domain publishers, each of whom operate according to their specific use cases for vulnerability identification and definition.

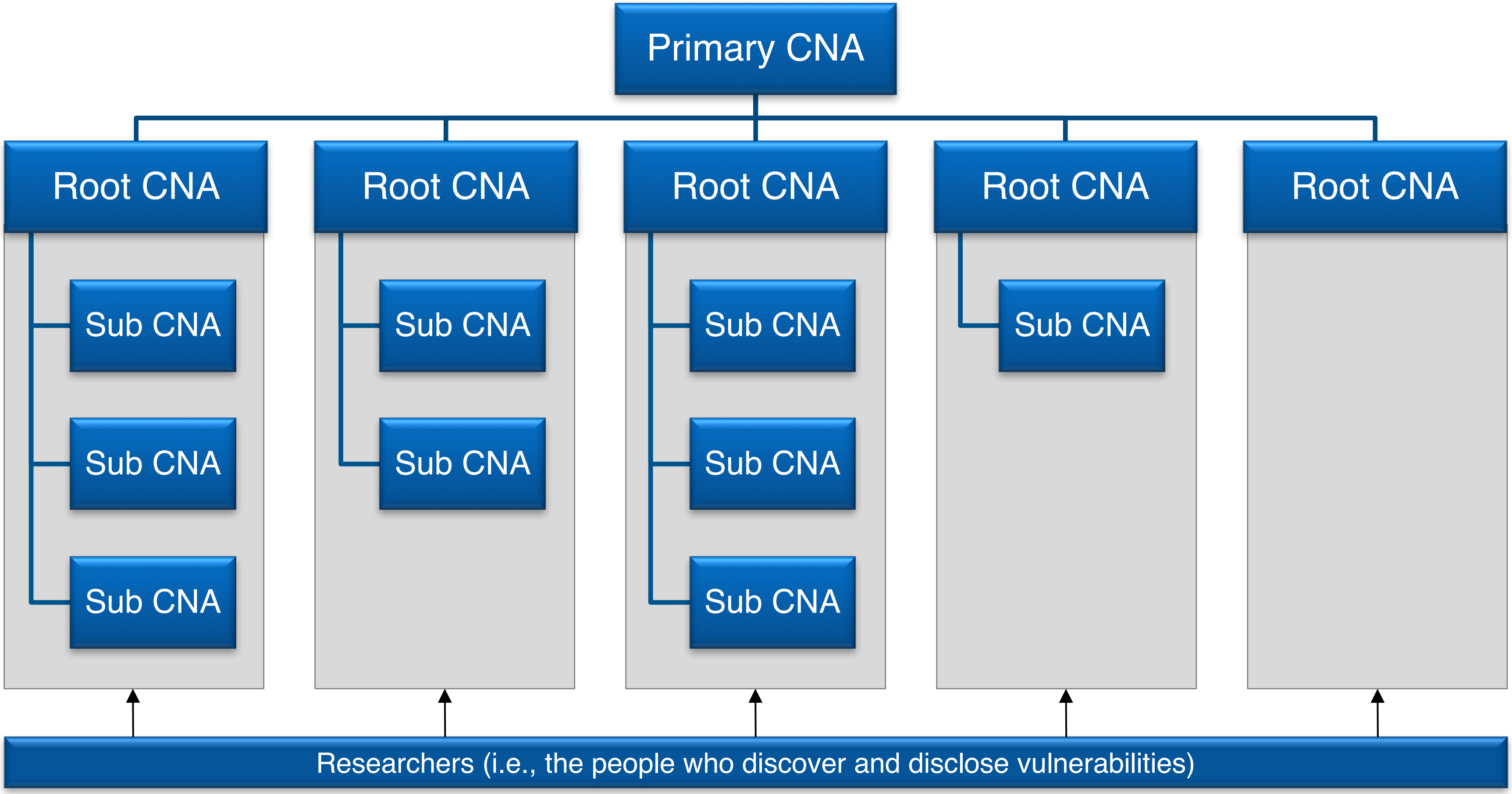
Challenges for the CVE Program

- **The CVE Program’s challenges**
  - Satisfy the demand for timely CVE ID assignments
  - Increase the number of CVE IDs to match the increasing rate of vulnerabilities
  - Expand the CVE Program’s scope to address the evolving state of vulnerability management
  - Expand CVE to domains beyond the Information Technology (IT) domain

Global Needs Related to CVE

- **The global community's needs:**
  - Unique vulnerability identification covering critical infrastructure and key resources within the IT sector and beyond.
  - A community of experts with committed participation in vulnerability management for each domain
  - A process for those experts to follow that ensures repeatability and support within and across domains
  - A means to evolve the processes to accommodate changes

Federated Hierarchy Today



Multi-Domain Challenges

- **Each CVE domain must review and decide on any customizations to the basic CVE governance structure**
  - Different regulatory, legal, and practical considerations within a domain will affect the requirements on a CVE domain's internal governance.

Vulnerability management practices and governance functions within a CVE domain must be established by that domain's community.

Federation allows for this need for flexibility and adaptability.

Participation in the CNA Program

Participation in the CNA Program

- **CNAs can be**
  - Software or hardware vendors
  - Vulnerability research organizations
  - Computer Emergency Response Teams (CERTs)/Computer Security Incident Response Teams (CSIRTs)
  - Technology domain authorities or groups
  - Others?
- **The CVE Program provides all CNAs with a set of documentation, including**
  - Rules and responsibilities
  - Operational guidelines
  - Policy and process templates
- **Individual CNAs have a specific scope and designated as a Root or Sub-CNA**

Participating as a CNA

- CNAs coordinate with their Root CNA or the Primary CNA to ensure the CNA analysts are properly trained, and all roles and responsibilities will be satisfied at an appropriate level of quality.
- The CVE Program provides various forums through which CNAs can collaborate with other CNAs within their domain and across the CNA program.
- There is no cost to participate in the CNA program beyond the internal operational costs of assigning CVE IDs and communicating with the CNA community and external disclosers.

To Participate in the CNA Program

To participate, contact any one of the following:

1. **The Primary CNA, MITRE, at:**
   - Web: http://cve.mitre.org/
   - Web: https://cveform.mitre.org/
   - Email: cve@mitre.org

2. **Members of the CVE Board**

3. **An existing CNA when considering becoming its Sub-CNA**

Questions

Contact CVE at cve@mitre.org

Or through http://cve.mitre.org

Twitter: @CVEannounce or @CVEnew

Vulnerability Definition

- A vulnerability in the context of the CVE Program, is defined as a weakness in the computational logic (e.g., code) found in software and some hardware components (e.g., firmware) that, when exploited, results in a negative impact to confidentiality, integrity, OR availability.

- Mitigation of the vulnerabilities in this context typically involve coding changes, but could also include specification changes, or even specification deprecations (e.g., removal of affected protocols or functionality in their entirety).