GCVE-BCP-03 - Decentralized Publication Standard

Contents

0.1 Decentralized Publication Standard

- **Version**: 1.1
- **Status**: Draft (for Public Review)
- **Date**: 2025-06-13
- **Authors**: GCVE Working Group
- **BCP ID**: BCP-03

0.1.1 Introduction

This document describes the decentralized publication model that allows GNAs to publish their vulnerability information directly, without relying on a centralized system.

It also outlines the access methods used by GNAs to distribute their published vulnerabilities through various mechanisms.

Clients can rely on this BCP document to obtain the vulnerabilities published by a GNA.

0.2 Mechanism

The decentralized model is based on the principle that each GNA has full control over its own publication process. The GCVE directory then provides a way to discover the entry points for collecting vulnerability information from your trusted set of GNAs, allowing users to decide whom to trust and from whom to pull vulnerability information.

0.2.1 Reference Implementation

A reference implementation is available in the open-source project Vulnerability-Lookup, which supports this BCP. It can be used both for decentralized publication and for collecting vulnerability information from all GNAs listed in the GCVE directory.

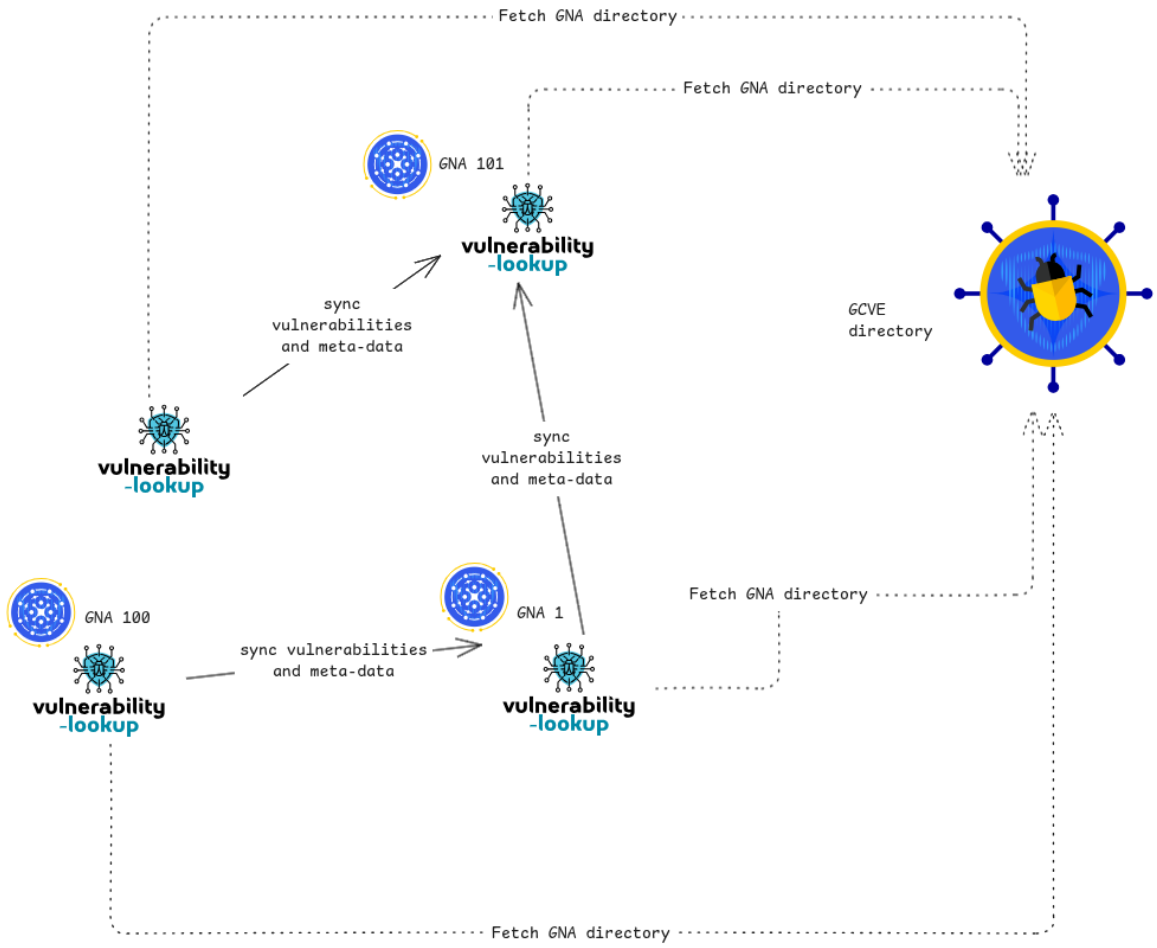

Figure 1: An overview of the GCVE decentralized publication model

0.3 Transport

The transport mechanism used to gather vulnerability information relies on HTTP, with two modes of access via a single URL. One mode is a simple REST API that allows retrieval of the latest published vulnerabilities—either starting from a specific date or by paginating through the entire dataset. The other mode is a static endpoint that serves a vulnerability file. A GNA can use one or both transport

methods.

The URL is referenced in the GCVE directory under the `gcve_pull_api` field.

0.3.1 HTTP ReST API

The API endpoint is defined in the field `gcve_pull_api`, which must support at least the following API endpoints:

- `/api/vulnerability/recent/` – Retrieves vulnerabilities reported after a specified date, with optional filters for source and number of results.
- `/api/vulnerability/last/` – Retrieves the latest vulnerabilities, with optional filters for source and number of results.

The full URL for each endpoint is constructed based on the value of the `gcve_pull_api` field from GCVE the directory.

0.3.2 Static File

The full URL of the static endpoint is constructed based on the value of the `gcve_pull_api` field from the GCVE directory.

- `/dumps/gna-{GCVE-ID}.ndjson` – A static dump of the vulnerabilities published by the GNA.

A `security.txt` file can be used to declare a GCVE publication endpoint using the `GCVE` field.

0.4 Format

GCVE-BCP-03 does not enforce a specific JSON format for vulnerability publication.

However, the recommended format—also used in the reference implementation—is the CVE Record Format, as described in https://github.com/CVEProject/cve-schema/blob/main/schema/CVE_Record_Format.json.

This BCP may be updated at a later stage to include a list of additional supported vulnerability formats.

0.5 Example Service

`GNA-1` provides a reference service that can be used to query and test a client.

- The API endpoint is available at: https://vulnerability.circl.lu/api/
- The static file is available at: https://vulnerability.circl.lu/dumps/gna-1.ndjson