GCVE-BCP-01 - Signature Verification of the Directory File

Contents

0.1 GCVE-BCP-01 - Signature Verification of the Directory File

- **Version**: 1.1
- **Status**: Published
- **Date**: 2025-04-26
- **Authors**: GCVE Working Group
- **BCP ID**: BCP-01

This guide is distributed and available under CC-BY-4.0.

Copyright (C) 2025 GCVE Initiative.

0.1.1 Abstract

This document defines the Best Current Practice (BCP) for verifying the cryptographic signature of the GCVE directory file.

The directory file contains authoritative metadata about GCVE Numbering Authorities (GNAs). To preserve trust and ensure integrity, all users must verify the digital signature of the file using the GCVE public key and a standardized OpenSSL verification method before using its content.

0.1.2 1. Scope and Purpose

The purpose of this BCP is to ensure that consumers of the GCVE directory file can cryptographically validate its authenticity and integrity before parsing or trusting its content. This procedure protects against tampering and unauthorized modifications of the directory file.

0.1.3 2. File and Signature Format

- The GCVE directory file is named: `directory.json` available in TLS at https://gcve.eu/dist/gcve.json

- The accompanying digital signature is a **base64-encoded SHA-512 signature**: `directory.json.sigsha512` available in TLS at https://gcve.eu/dist/gcve.json.sigsha512
- The GCVE signing public key is available at: https://gcve.eu/dist/key/public.pem, the public key is also available as a TXT record in `_key.GCVE.eu` (`dig -t TXT _key.gcve.eu`).

0.1.4 3. Signature Verification Method

0.1.4.1 3.1 Prerequisites

- OpenSSL installed on your system.
- The GCVE public key https://gcve.eu/dist/key/public.pem.
- Access to the directory file and its `.sigsha512` signature file.

0.1.4.2 3.2 Verification Script

To streamline verification, the following example script can be used https://github.com/gcve-eu/gcve-eu-tools/blob/main/sign/verify.sh.

```
bash verify.sh /home/yourusername/git/gcve.eu-directory/gcve.json /home/yourusername/git/gcve.eu-directory/gcve.json.sigsha512
Verified OK
```

0.1.4.3 3.3 Python Library

The GCVE Python client includes a command to locally retrieve the GNA registry and verify its integrity.

```
gcve registry --pull
Pulling from registry...
Downloaded updated https://gcve.eu/dist/key/public.pem to data/public.pem
Downloaded updated https://gcve.eu/dist/gcve.json.sigsha512 to data/gcve.json.sigsha512
Downloaded updated https://gcve.eu/dist/gcve.json to data/gcve.json
Integrity check passed successfully.
```

More information in the documentation of the client.

0.1.5 4. Automation and Integration

- Include signature verification in CI/CD pipelines and data ingestion workflows.
- Automatically fetch the latest trusted public key from: https://gcve.eu/dist/key/public.pem
- Trigger alerts or reject workflows if signature verification fails.

0.1.6 5. Key Management and Security

- The GCVE signing key is securely stored and only accessible to authorized personnel at CIRCL, where GCVE.eu is operated.
- Any key rollover events will be clearly announced and accompanied by signed transition documentation.
- Additional signing methods may be added depending on the evolution of best practices in cryptographic algorithms.
- Consumers should monitor the GCVE website for updates or revocations of the signing key.

0.1.7 6. License

This document is released under the Creative Commons Attribution 4.0 International License (CC-BY 4.0).