GCVE-BCP-09 - Scope of a GCVE Record

GCVE.eu

GCVE.eu

Contents

1 GCVE-BCP-09: Scope of a GCVE Record

- **Version**: 1.0
- **Status**: Draft (for Public Review)
- **Date**: 2026-05-20
- **Authors**: GCVE Working Group
- **BCP ID**: BCP-09

1.1 Abstract

This document clarifies what is actually recorded in GCVE. A GCVE record is not limited to the traditional concept of a vulnerability description. In the GCVE model, records are assigned independently by a GCVE Numbering Authority (GNA) and may represent a broader set of vulnerability-related information.

A GCVE record may describe a vulnerability in software, hardware, firmware, infrastructure, or cloud services. It may also represent clarification, remediation, contextualization, correlation, or other vulnerability-related information published under the authority and according to the data model of a GNA.

This document defines the scope of a GCVE record and provides guidance for GNAs and consumers so that decentralized publication remains interoperable while preserving the freedom of GNAs to define records according to their operational reality.

1.2 Status of This Memo

This memo is a proposal for the GCVE Best Current Practice series.

1.3 Introduction

Traditional vulnerability identification systems are often understood as assigning an identifier to a short description of a software vulnerability. That model has historically been useful, but it is too narrow for modern vulnerability management and coordinated disclosure.

In operational practice, security-relevant records may concern more than a single classical software flaw. Vulnerability information may concern:

- software vulnerabilities;
- vulnerabilities in cloud or managed services;
- downstream impact statements;
- configuration-dependent exposure;
- remediation or mitigation guidance;
- clarifications related to an existing vulnerability record;
- authoritative records that refine, update, or contextualize another published record.

GCVE is intentionally designed to support a decentralized model. GCVE records are assigned independently by GNAs. As a consequence, the meaning and scope of a record are not restricted to a legacy notion of a vulnerability entry. A GCVE record is better understood as a record of vulnerability-related information, whose precise semantics are determined by the GNA that assigned it.

This document describes that broader interpretation and establishes best current practices for publication and consumption.

1.4 Terminology

The key words **MUST**, **MUST NOT**, **SHOULD**, **SHOULD NOT**, and **MAY** in this document are to be interpreted as described in RFC 2119 and RFC 8174.

1.4.1 GCVE Record

A **GCVE record** is a vulnerability-related information object identified by a GCVE identifier and assigned by a GNA.

1.4.2 GNA

A **GCVE Numbering Authority (GNA)** is an entity authorized to assign GCVE identifiers and publish associated records according to its own scope, governance, and data model.

1.4.3 Vulnerability-Related Information

Vulnerability-related information is information materially relevant to the identification, description, clarification, correlation, impact analysis, remediation, or contextualization of a vulnerability or exposure.

1.4.4 Record Model

A **record model** is the set of semantics, structure, categories, and rules used by a GNA to define the kinds of GCVE records it issues.

1.5 Problem Statement

A common assumption is that every vulnerability identifier corresponds to one canonical description of one software flaw. This assumption creates several problems:

1. It does not reflect the reality of cloud services and hosted environments.
2. It does not provide a natural place for clarification or correction records.
3. It does not fit downstream or constituency-specific impact statements.
4. It does not account for remediation-centered or relationship-centered records.
5. It forces different operational needs into a narrow data model.

GCVE addresses this by allowing a GCVE record to represent more than a classical vulnerability description. The scope of the record is defined by the assigning GNA and its model, not by a fixed legacy assumption.

1.6 Core Principle

A GCVE record is a **GNA-assigned record about vulnerability information**.

A GCVE record **MUST NOT** be interpreted as being limited to a traditional vulnerability description.

The semantics of a GCVE record are determined by:

- the assigning GNA;
- the GNA's published record model;
- the content of the record itself;
- the relationships the record declares with other records.

Consumers **MUST NOT** assume that all GCVE records are identical in nature or purpose. Consumers **SHOULD** interpret a GCVE record according to the GNA context in which it was issued.

1.7 Scope of a GCVE Record

A GCVE record **MAY** represent any of the following, provided it remains within the scope of vulnerability-related information as defined by the assigning GNA.

1.7.1 Vulnerability Description

A GCVE record may describe a vulnerability in software, hardware, firmware, or infrastructure.

Examples include:

- a memory corruption vulnerability in a library;
- an authentication bypass in a web application;
- an authorization flaw in a management interface;
- an insecure default behavior in an appliance.

1.7.2 Cloud or Service Vulnerability

A GCVE record may describe a vulnerability or security weakness in a cloud service, hosted platform, SaaS environment, or managed service.

This is especially important where the affected object is not a distributable software package and does not fit traditional version-oriented models.

1.7.3 Clarification Record

A GCVE record may exist primarily to clarify a previously published vulnerability record.

Examples include:

- narrowing or expanding affected scope;
- correcting an exploitation precondition;
- clarifying impact or severity;
- explaining why a record does not apply to a specific environment;
- documenting ambiguity or disputed interpretation.

A clarification record is a valid GCVE record because clarification is part of vulnerability information.

1.7.4 Remediation or Mitigation Record

A GCVE record may focus on remediation, mitigation, workarounds, containment, or recovery information tied to a vulnerability or set of vulnerabilities.

This may include:

- authoritative patch guidance;
- specific remediation constraints;
- mitigation instructions for managed environments;
- records documenting the operational resolution of a vulnerability condition.

1.7.5 Product-, Vendor-, or Deployment-Specific Record

A GCVE record may capture how a vulnerability applies in a specific downstream product, distribution, service configuration, or operational deployment.

Examples include:

- a downstream vendor record concerning an upstream vulnerability;
- a distribution-specific impact statement;
- a service-operator record indicating exposure only in a certain deployment mode.

1.7.6 Relationship or Context Record

A GCVE record may exist to express an important relationship between vulnerability facts or other records.

Examples include:

- one record superseding another;
- one record refining another;
- a record collecting authoritative context about a previously disclosed issue;
- a record documenting that multiple externally referenced issues correspond to one operational problem.

1.7.7 Other Vulnerability Information Defined by the GNA

A GNA **MAY** define additional categories of GCVE records, as long as those records remain meaningfully related to vulnerability information and are documented in the GNA's model.

1.8 Boundary of What Can Be Recorded

The practical boundary of what may be recorded in GCVE is the **GNA model**.

This means:

- GCVE does not impose a single universal semantic category for all records.
- A GNA may define the kinds of records it issues according to its mission and constituency.
- The assigning GNA is responsible for ensuring that the issued records remain within a vulnerability-information context.

A GNA **SHOULD NOT** use GCVE to publish records that are unrelated to vulnerability information merely because the system permits flexible modeling.

GCVE flexibility exists to support real-world decentralization, not semantic arbitrariness.

1.9 Requirements for GNAs

1.9.1 Publish Clear Semantics

A GNA **SHOULD** document the categories of GCVE records it assigns and the meaning of those categories.

At minimum, a GNA **SHOULD** document:

- what kinds of records it issues;
- what each type means;
- whether records describe original findings, clarifications, remediation, or contextual statements;
- how records relate to one another;
- what consumers may safely infer from a record.

1.9.2 Preserve Authority and Scope

Each GCVE record **SHOULD** express a meaningful vulnerability-related statement under the authority of the assigning GNA.

A GNA **MUST** ensure that the record remains within its declared scope and governance.

1.9.3 Use Explicit Relationships

When one GCVE record clarifies, updates, supersedes, narrows, references, or contextualizes another record, the GNA **SHOULD** express that relationship explicitly where the data model allows it.

This improves machine processing and avoids ambiguity for consumers.

1.9.4 Avoid False Uniformity

A GNA **SHOULD NOT** force all records to appear as classical vulnerability descriptions if doing so reduces precision or hides the actual meaning of the record.

Explicit semantics are preferable to misleading uniformity.

1.9.5 Support Modern Environments

A GNA **MAY** issue records for cloud services, hosted platforms, or operational environments even when those do not map cleanly to traditional product/version vulnerability descriptions.

1.10 Evaluation for GNA

GCVE preserves the full autonomy of each GNA. A GNA remains free to define its own operational model, disclosure philosophy, review process, publication scope, and record model according to its constituency, legal constraints, and mission. BCP-06 is explicitly designed to support this diversity: it does not impose uniform behavior or privilege a single publication model, but instead provides a common framework to describe those operational characteristics in a transparent and machine-readable way.

Nevertheless, that autonomy does not prevent public accountability. BCP-06 allows the GCVE directory to publish conformance fields, scoring elements, and evaluation criteria so that a GNA's posture can be assessed publicly and consistently. In that model, the directory does not act as a central approval authority; it acts as a transparency layer that can expose declared practices, measurable criteria, and public evaluations following BCP-06.

1.11 Requirements for Consumers

1.11.1 Do Not Assume Legacy Semantics

Consumers **MUST NOT** assume that every GCVE record corresponds to a single, traditional vulnerability description as typically used in centralized vulnerability publication models. Consumers **SHOULD** instead interpret each record according to the assigning GNA, its declared scope, and its record model.

1.11.2 Interpret Records in GNA Context

Consumers **SHOULD** interpret records according to:

- the assigning GNA;
- the record category or type;
- the stated scope;
- the relationships to other records;
- the record content itself.

1.11.3 Preserve Provenance

Consumers **SHOULD** preserve provenance information, including:

- assigning GNA;
- publication date;
- update history if available;
- references and relationships;
- status and scope indicators.

1.11.4 Avoid Over-Aggressive Normalization

Consumers **SHOULD NOT** collapse multiple GCVE records into one purely because they appear related.

Different records may represent different authoritative views or different aspects of the same vulnerability situation.

1.11.5 Support Heterogeneous Records

Consumers **SHOULD** be prepared to ingest records that are not pure vulnerability descriptions, including clarification, remediation, and service-specific records.

1.12 Recommended Interpretation Model

For interoperability, a consumer should be able to answer the following questions for any GCVE record:

1. **Who assigned this record?**
2. **What kind of vulnerability-related information does it represent?**
3. **What is the scope of the statement?**
4. **Does it describe, clarify, remediate, or contextualize something?**
5. **How does it relate to other records?**
6. **What can and cannot be inferred from it?**

If a consumer cannot answer these questions from the record alone, it should consult the GNA's published model.

1.13 Examples

The following examples are illustrative.

1.13.1 Classical Software Vulnerability

A GNA assigns a GCVE record to a remote code execution vulnerability in a library. This is a valid and expected GCVE record.

1.13.2 Cloud Service Issue

A cloud provider assigns a GCVE record to an authorization weakness in a managed API. There is no installable package version exposed to customers, but the record is still valid because it describes vulnerability-related information.

1.13.3 Clarification of Another Record

A downstream vendor assigns a GCVE record stating that a previously referenced issue does not affect its distribution because a vulnerable feature is not enabled. This is a valid GCVE record because it provides authoritative clarification.

1.13.4 Remediation-Centered Record

A managed service operator assigns a GCVE record focused on mitigation steps and operational containment for a known exposed service condition. This is a valid GCVE record because remediation is part of vulnerability information.

1.13.5 Contextual Record

A GNA publishes a record linking several related advisories and clarifying that they refer to one underlying vulnerability condition. This is a valid contextual GCVE record.

1.14 Interoperability Considerations

GCVE does not require all records to be semantically identical. Interoperability comes from explicit meaning, not forced sameness.

To support interoperability:

- GNAs **SHOULD** document their record model;
- records **SHOULD** expose relationships where possible;
- consumers **SHOULD** preserve type and provenance;
- mappings to other ecosystems **MAY** be performed, but any semantic loss **SHOULD** be acknowledged.

Systems integrating GCVE should understand that some GCVE records map naturally to traditional vulnerability entries, while others may map more naturally to advisories, statements, remediation objects, or contextual records.

1.15 Security Considerations

Poor interpretation of GCVE record semantics may create security risks.

Examples include:

- treating a clarification as a new vulnerability;
- treating a remediation record as proof of universal remediation;
- generalizing a deployment-specific record to all environments;
- ignoring GNA scope and provenance.

GNAs should minimize ambiguity by documenting their model and using explicit relationships. Consumers should minimize ambiguity by preserving provenance and avoiding simplistic assumptions.

1.16 Operational Considerations

The value of GCVE lies in decentralized publication without unnecessary semantic restriction.

Modern vulnerability coordination involves many actors, including software vendors, cloud providers, downstream integrators, CSIRTs, infrastructure operators, and sector-specific authorities. These actors do not always need to publish the same kind of record.

GCVE therefore supports a broader concept: a GCVE record is an authoritative vulnerability-information record whose boundaries are determined by the GNA model.

This flexibility is not a weakness. It is a necessary design property for a decentralized vulnerability information ecosystem.

1.17 Summary of Best Current Practice

The following is the best current practice defined by this document:

- A GCVE record is a GNA-assigned record of vulnerability-related information.
- A GCVE record is not limited to a traditional vulnerability description.
- GCVE records may cover software, hardware, firmware, cloud services, clarifications, remediation, contextualization, and other vulnerability-related statements.
- The practical boundary of what can be recorded is defined by the GNA model.
- GNAs should document their record semantics clearly.
- Consumers must not assume that every GCVE record follows the traditional vulnerability-description model used in centralized publication systems.

1.18 Conclusion

GCVE is designed to support decentralized and realistic vulnerability publication. Restricting GCVE records to the narrow idea of a classical vulnerability description would not reflect current operational needs.

A GCVE record should therefore be understood as a flexible but authoritative vulnerability-information record issued independently by a GNA. It may describe a vulnerability directly, clarify another record, provide remediation context, document service-specific exposure, or represent other vulnerability-related information defined by the GNA model.

That broader understanding is essential to the GCVE design and should be treated as best current practice.

2 Acknowledgements

2.1 BCP-09 Coordinator

- Team GCVE - BCP-09 Coordination