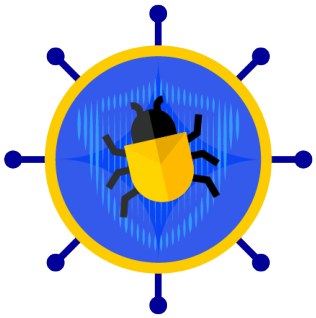
GCVE-BCP-07 - Known Exploited Vulnerability - KEV Assertion Format

GCVE.eu

GCVE.eu

Contents

1 Known Exploited Vulnerability - KEV Assertion Format



GCVE.eu

- **Version**: 1.8
- **Status**: Draft (for Public Review)
- **Date**: 2026-02-04
- **Authors**: GCVE Working Group
- **BCP ID**: BCP-07

2 Introduction

Known Exploited Vulnerabilities (KEVs) have become a critical signal for vulnerability prioritization, operational risk management, and policy-driven remediation. Governments, CSIRTs, and sectoral authorities increasingly rely on KEV lists to mandate patching, trigger incident response, or inform compliance decisions. However, existing KEV publications are largely list-based and opaque, often asserting exploitation without clearly expressing who made the claim, when exploitation was observed versus declared, what type of evidence supports it, where it was seen, or with what level of confidence. As KEV data is increasingly consumed by automated systems and cross-border information-sharing mechanisms, the absence of structured, contextual metadata limits interoperability, trust calibration, and analytical reuse.

This Best Current Practice defines a standardized KEV assertion format that preserves the intentionally simple and binary nature of KEV while adding minimal but essential context. Within the GCVE or other ecosystem, where vulnerabilities may be disclosed and referenced by multiple independent authorities, exploitation claims must be clearly distinguishable from vulnerability identifiers and treated as attributable statements rather than universal truths. The format enables multiple, potentially conflicting assertions to coexist, supports explicit attribution and confidence signaling, and facilitates interoperability with existing vulnerability, CSIRT, and policy ecosystems without turning KEV into full threat intelligence or requiring disclosure of sensitive evidence.

3 Known Exploited Vulnerability - KEV Assertion Format

This format describes a **generic KEV (Known Exploited Vulnerability) assertion format**.

The goal is to express *who claims exploitation*, *when*, *based on what*, *where it was observed*, and *with which level of confidence*, without turning KEV into full threat intelligence. A KEV assertion is usually very binary and lacking some meta-information. The format adds some information which could better capture details about the exploitation. A majority of the fields are optional except `vulnerability`, `status` and `evidence.[].source` which are recommended.

3.1 Usage Consideration

KEV and CVE (or GCVE) represent different layers in the model, and that distinction is intentional.

A vulnerability identifier (CVE/GCVE) is primarily about establishing the identity of a vulnerability something that the ecosystem can refer to consistently over time. KEV, on the other hand, is an assertion about observed exploitation activity, made by an observer at a given point in time. In an ideal world, the same actor that defines the vulnerability (for example, a vendor CNA) would also confirm exploitation, but in practice these concerns are frequently dissociated.

There are several common situations where vulnerability identity and exploitation assertions do not originate from the same place or even at the same time:

- Embargoed or restricted vulnerabilities, where exploitation is observed and tracked within a limited circle (CSIRTs, intelligence teams, trusted communities) before public disclosure or before a vendor-assigned identifier exists.
- Situations of disagreement or asymmetry of knowledge, where an observer has high-confidence evidence of exploitation while the vendor disputes impact, scope, or even the existence of the vulnerability.
- Early or partial observations, where exploitation activity is detected before a stable understanding of affected products, attack vectors, or vulnerability class has been established.

The KEV format explicitly models exploitation as an event-level assertion linked to a vulnerability identity, rather than as part of the identity itself. This reflects operational reality: exploitation is something that happens, may occur multiple times, may be observed by different parties, and may be interpreted differently as more information becomes available.

This separation already exists implicitly across today's KEV lists, vendor advisories, and threat intelligence reports, but it is inconsistently expressed, often duplicated, and rarely machine-parseable in a coherent way. The GCVE KEV format (BCP-07) provides a structured and open way to express these assertions while anchoring them to a shared vulnerability identifier when one exists.

Importantly, KEV entries are assertions, not ground truth.

They may later be revised, withdrawn, or contradicted by other observers. Decoupling identity from assertions allows such evolution without disconnecting from the underlying vulnerability record. A vulnerability identity should remain stable even if claims about exploitation change over time.

This model also assumes that multiple assertions per vulnerability identity are normal and expected. Different organisations may publish different KEV entries, CVSS scores, or detection signatures for the same GCVE ID, reflecting different perspectives, evidence sets, or confidence levels. Centralising identity while allowing plural assertions enables this diversity in a federated model.

With respect to identity-related data (such as vendor, product, or RCE status), once a vulnerability identity is established and assigned a GCVE ID, CVE ID (or any id), that identity should be the container for stable characteristics from a vendor. Assertions such as KEV entries, CVSS vectors, or signatures should primarily reference the GCVE ID, CVE ID (or any id) and focus on what is specific to the assertion itself: context, timing, confidence, evidence, or scoring rationale. The goal is not to repeat identity-defining attributes in every assertion.

Finally, this separation is essential for machine-readability. Clear boundaries between identity and assertions enable automated correlation, reasoning, and downstream decision-making across heterogeneous data sources. GCVE KEV (BCP-07) treats exploitation knowledge as structured data, without overloading the vulnerability identity layer itself.

3.2 Format

It's a single JSON object (ECMA 404) per KEV entry. The KEV entry is associated to a vulnerability ID in GCVE ID or any known vulnerability identifier.

3.2.1 Sample

3.2.1.1 Combined KEV Assertion

The JSON file below provides an example of a KEV file referencing a GCVE vulnerability ID.

```
{
"vulnerability": {
    "vulnId": "GCVE-0-2025-55182"
  },
 "status": {
    "exploited": true,
    "status_reason": "confirmed",
    "status_updated_at": "2025-12-24T10:15:00Z"
  },
 "characteristics": {
    "remote_code_execution": true,
    "authentication_required": false,
    "local_access_required": false
  },
 "timestamps": {
    "first_seen_at": "2025-12-03T10:15:00Z",
    "asserted_at": "2025-12-05T12:10:11Z",
    "recorded_at": "2025-12-05T13:15:00Z",
    "last_seen_at": "2025-12-24T09:42:21Z"
  },
 "scope": {
    "observation_regions": ["Europe", "North America"],
    "victim_countries": ["LU","BE", "US", "CA"],
    "sector": ["Telecoms", "Aerospace"],
    "asset_exposure": ["internet-facing"],
    "notes": "Regions reflect observed evidence, not global exclusivity
       ."
  },
"evidence": [
    {
      "type": "incident_response",
      "signal": "confirmed_compromise",
      "confidence": 0.9,
      "source": "national-csirt",
      "details": {
        "observed_outcome": ["initial-access", "rce"],
        "detection_basis": ["forensics", "log-analysis"]
      }
    },
    {
      "type": "honeypot",
      "signal": "in_the_wild_attempts",
      "confidence": 0.6,
      "source": "research-honeynet",
```

```
      "details": {
        "attempt_volume": "high",
        "successful_exploitation": false
      }
    }
  ],
  "references": [
    {
      "id": "GCVE-0-2025-55182",
      "url": "https://vulnerability.circl.lu/vuln/CVE-2025-55182#
         sightings"
    }
  ],
}
```

3.2.1.2 CISA KEV in BCP-07 Format

The JSON file below provides an example of a KEV file referencing a CISA KEV assertion.

```
{
  "vulnerability": {
    "vulnId": "CVE-2020-29583"
  },
  "status": {
    "exploited": true,
    "status_reason": "confirmed",
    "status_updated_at": "2021-11-03T00:00:00Z"
  },
  "timestamps": {
    "first_seen_at": "2021-11-03T00:00:00Z",
    "asserted_at": "2021-11-03T00:00:00Z",
    "recorded_at": "2026-01-22T05:07:44Z"
  },
  "evidence": [
    {
      "type": "vendor_report",
      "signal": "successful_exploitation",
      "confidence": 0.8,
      "source": "cisa-kev",
      "details": {
        "feed": "CISA Known Exploited Vulnerabilities Catalog",
        "date_added": "2021-11-03",
        "due_date": "2022-05-03",
        "vendorProject": "Zyxel",
        "product": "Multiple Products",
        "vulnerabilityName": "Zyxel Multiple Products Use of Hard-Coded
            Credentials Vulnerability",
        "knownRansomwareCampaignUse": "Unknown",
        "cwes": [
```

```
            "CWE-522"
          ]
        }
      }
    ],
    "references": [
      {
        "id": "CVE-2020-29583",
        "url": "https://www.cisa.gov/known-exploited-vulnerabilities-
           catalog?search_api_fulltext=CVE-2020-29583"
      }
    ],
    "scope": {
      "notes": "KEV entry: Zyxel Multiple Products Use of Hard-Coded
         Credentials Vulnerability | Affected: Zyxel / Multiple Products
         | Description: Zyxel firewalls (ATP, USG, VM) and AP Controllers
          (NXC2500 and NXC5500) contain a use of hard-coded credentials
         vulnerability in an undocumented account (\"zyfwp\") with an
         unchangeable password. | Required action: Apply updates per
         vendor instructions. | Due date: 2022-05-03 | Known ransomware
         campaign use (KEV): Unknown | Notes (KEV): https://nvd.nist.gov/
         vuln/detail/CVE-2020-29583"
    }
}
```

3.2.2 Field Description

3.2.2.1 `vulnerability` Object

Describes the vulnerability being asserted as exploited.

3.2.2.1.1 `vulnerability.vulnId`

- **Type:** string
- **Required:** yes
- **Description:** GCVE, CVE identifier, GHSA or any identifier of the vulnerability.
- **Example:** `"GCVE-0-2025-55182"`

3.2.2.1.2 `vulnerability.altId`

- **Type:** array
- **Required:** no
- **Description:** Alternative identifiers that refer to the same vulnerability, used in addition to `vulnerability.vulnId`.

3.2.2.2 `status` Object

Represents the current exploitation status.

3.2.2.2.1 `status.exploited`

- **Type:** boolean
- **Description:** Indicates whether exploitation has been observed or asserted.
- **Semantics:** Does not imply global prevalence or universal exploitability.

3.2.2.2.2 `status.status_reason`

- **Type:** string (enum)
- **Allowed values:** `confirmed`, `suspected`, `disputed`, `historical`, `unknown`
- **Description:** Rationale behind the exploitation status.

3.2.2.2.3 `status.status_updated_at`

- **Type:** string (RFC3339 datetime)
- **Description:** Timestamp of the last change to the exploitation status in the KEV assertion.

3.2.2.3 `characteristics` Object

Describes high-level technical characteristics of the vulnerability that are relevant to exploitation assessment, without providing exploit details or turning the KEV assertion into full threat intelligence.

These fields describe properties of the vulnerability itself, not necessarily every observed exploitation instance.

3.2.2.3.1 `characteristics.remote_code_execution`

- **Type:** boolean
- **Description:** Indicates whether successful exploitation can result in remote code execution.
- **Notes:** Does not imply exploit reliability or ease of weaponization.

3.2.2.3.2 `characteristics.authentication_required`

- **Type:** boolean
- **Description:** Indicates whether authentication is required to exploit the vulnerability.
- **Notes:** Reflects the weakest known exploitation path.

3.2.2.3.3 `characteristics.local_access_required`

- **Type:** boolean
- **Description:** Indicates whether local system access is required prior to exploitation.
- **Notes:** Useful to distinguish remote exploitation from post-compromise privilege escalation.

3.2.2.3.4 `characteristics.severity`

- **Type:** number (0.0–100)
- **Description:** Severity associated with this vulnerability.

3.2.2.4 `timestamps` Object

Separates different notions of time to avoid ambiguity.

3.2.2.4.1 `timestamps.first_seen_at`

- **Type:** string (RFC3339 datetime)
- **Description:** Earliest known exploitation activity based on technical observation.
- **Notes:** May be estimated and updated retroactively.

3.2.2.4.2 `timestamps.asserted_at`

- **Type:** string (RFC3339 datetime)
- **Description:** Date when an authority or source officially declared exploitation.
- **Notes:** Mirrors fields such as “date added” in KEV lists.

3.2.2.4.3 `timestamps.recorded_at`

- **Type:** string (RFC3339 datetime)
- **Description:** Timestamp when this assertion was ingested or recorded by the collector.
- **Notes:** System-specific and independent of the source.

3.2.2.4.4 `timestamps.last_seen_at`

- **Type:** string (RFC3339 datetime)
- **Description:** Most recent confirmed observation of exploitation activity.
- **Notes:** Optional and often unavailable.

3.2.2.5 `scope` Object

Defines the observed context of exploitation.

3.2.2.5.1 `scope.observation_regions`

- **Type:** array of strings
- **Description:** Geographic regions where exploitation evidence was observed. The region can be described in **UN M49** format to facilitate automation.
- **Notes:** Reflects sensor or reporting coverage, not global limits.

3.2.2.5.2 `scope.victim_countries`

- **Type:** array of strings
- **Description:** Countries in ISO 3166 where confirmed victims were identified.
- **Notes:** Often incomplete or unavailable.

3.2.2.5.3 `scope.sector`

- **Type:** array of strings
- **Description:** Sectors targeted or affected by exploitation. The sector **SHALL** come from the MISP galaxy sector.
- **Example:** `"Telecoms"`, `"Aerospace"`

3.2.2.5.4 `scope.asset_exposure`

- **Type:** array of strings
- **Allowed values:** `internet-facing`, `internal`, `vpn-accessible`, `unknown`
- **Description:** Exposure context of affected assets.

3.2.2.5.5 `scope.notes`

- **Type:** string
- **Description:** Human-readable clarifications to prevent misinterpretation.

3.2.2.6 `evidence` Array

Collection of independent signals supporting the exploitation claim.

3.2.2.6.1 `evidence[].type`

- **Type:** string (enum)
- **Allowed values:** `incident_response`, `telemetry`, `honeypot`, `sinkhole`, `vendor_report`, `public_report`, `research_report`, `unknown`
- **Description:** Origin of the exploitation evidence.

3.2.2.6.2 `evidence[].signal`

- **Type:** string (enum)
- **Allowed values: (can be multiple)** `in_the_wild_attempts`, `successful_exploitation`, `confirmed_compromise`, `mass_scanning`, `weaponized_exploit_available`
- **Description:** Nature of the observed exploitation signal.

3.2.2.6.3 `evidence[].confidence`

- **Type:** number (0.0–1.0) or enum
- **Description:** Confidence level associated with this evidence.

3.2.2.6.4 `evidence[].source`

- **Type:** string
- **Description:** Logical identifier of the reporting entity or data source. MISP org UUID? What about existing KEV source like CISA, ENISA or alike. Should we have an enum with existing ones? The source would be the only required fields has many KEV like the type of signal.

3.2.2.6.5 `evidence[].details`

- **Type:** object
- **Description:** Structured, free-form metadata describing how the signal was derived. Additional feeds from KEV sources which are not described in this format such as `cwes`.
- **Notes:** Content is implementation-specific.

3.2.2.6.6 `evidence[].gcve`

- **Type:** object
- **Description:** Structured object describing evidence originating from the GCVE ecosystem.

gcve Object

- `evidence[].gcve.vluuid`
  - **Type:** string
  - **Description:** UUID of the Vulnerability-Lookup instance where the assertion originated. If the UUID must be derived from a source other than Vulnerability-Lookup, GCVE maintains a list of known KEVs to determine the correct source UUID.
- `evidence[].gcve.gna`
  - **Type:** number (0–65535)
  - **Description:** GNA ID identifying the origin of the assertion.
- `evidence[].gcve.object_uuid`
  - **Type:** string
  - **Description:** UUID of the assertion associated with this evidence in the GCVE ecosystem.

3.2.3 JSON Schema

JSON Schema - GCVE-BCP-07 Known Exploited Vulnerability (KEV) Assertion Format.

```
{
  "$schema": "https://json-schema.org/draft/2020-12/schema",
  "$id": "https://gcve.eu/schemas/bcp-07-kev-assertion.schema.json",
  "title": "GCVE-BCP-07 Known Exploited Vulnerability (KEV) Assertion",
  "type": "object",
  "additionalProperties": false,
  "required": ["vulnerability", "status"],
  "properties": {
    "vulnerability": {
      "type": "object",
      "additionalProperties": false,
      "required": ["vulnId"],
      "properties": {
        "vulnId": {
          "type": "string",
          "description": "GCVE, CVE, GHSA or any identifier of the
             vulnerability."
        },
        "altId": {
          "type": "array",
          "description": "Alternative identifiers that refer to the
             same vulnerability, used in addition to vulnerability.
             vulnId.",
          "items": { "type": "string" }
        }
```

```
      }
    },

    "status": {
      "type": "object",
      "additionalProperties": false,
      "properties": {
        "exploited": {
          "type": "boolean",
          "description": "Indicates whether exploitation has been
              observed or asserted."
        },
        "status_reason": {
          "type": "string",
          "description": "Rationale behind the exploitation status.",
          "enum": ["confirmed", "suspected", "disputed", "historical",
              "unknown"]
        },
        "status_updated_at": {
          "type": "string",
          "format": "date-time",
          "description": "Timestamp of the last change to the
              exploitation status in the KEV assertion (RFC3339)."
        }
      }
    },

    "characteristics": {
      "type": "object",
      "additionalProperties": false,
      "description": "High-level technical characteristics relevant to
          exploitation assessment.",
      "properties": {
        "remote_code_execution": {
          "type": "boolean",
          "description": "Whether successful exploitation can result in
              remote code execution."
        },
        "authentication_required": {
          "type": "boolean",
          "description": "Whether authentication is required to exploit
              the vulnerability."
        },
        "local_access_required": {
          "type": "boolean",
          "description": "Whether local system access is required prior
              to exploitation."
        },
        "severity": {
          "type": "number",
          "minimum": 0.0,
```

```
            "maximum": 100.0,
            "description": "Severity associated with this vulnerability - (0.0100)."
          }
        }
      },

      "timestamps": {
        "type": "object",
        "additionalProperties": false,
        "description": "Separate notions of time to avoid ambiguity.",
        "properties": {
          "first_seen_at": {
            "type": "string",
            "format": "date-time",
            "description": "Earliest known exploitation activity based on technical observation (RFC3339)."
          },
          "asserted_at": {
            "type": "string",
            "format": "date-time",
            "description": "Date when an authority or source officially declared exploitation (RFC3339)."
          },
          "recorded_at": {
            "type": "string",
            "format": "date-time",
            "description": "Timestamp when this assertion was ingested/recorded by the collector (RFC3339)."
          },
          "last_seen_at": {
            "type": "string",
            "format": "date-time",
            "description": "Most recent confirmed observation of exploitation activity (RFC3339)."
          }
        }
      },

      "scope": {
        "type": "object",
        "additionalProperties": false,
        "description": "Observed context of exploitation.",
        "properties": {
          "observation_regions": {
            "type": "array",
            "description": "Geographic regions where exploitation evidence was observed (optionally UN M49).",
            "items": { "type": "string" }
          },
          "victim_countries": {
```

```
112             "type": "array",
113             "description": "Countries (ISO 3166) where confirmed victims
                    were identified.",
114             "items": {
115               "type": "string",
116               "minLength": 2,
117               "maxLength": 2
118             }
119           },
120           "sector": {
121             "type": "array",
122             "description": "Sectors targeted/affected (SHALL come from
                    MISP galaxy sector).",
123             "items": { "type": "string" }
124           },
125           "asset_exposure": {
126             "type": "array",
127             "description": "Exposure context of affected assets.",
128             "items": {
129               "type": "string",
130               "enum": ["internet-facing", "internal", "vpn-accessible", "
                      unknown"]
131             }
132           },
133           "notes": {
134             "type": "string",
135             "description": "Human-readable clarifications to prevent
                    misinterpretation."
136           }
137         }
138       },
139
140       "evidence": {
141         "type": "array",
142         "description": "Collection of independent signals supporting the
                exploitation claim.",
143         "items": { "$ref": "#/$defs/evidenceItem" }
144       },
145
146       "references": {
147         "type": "array",
148         "description": "Links/IDs referencing external resources about
                the vulnerability or sightings.",
149         "items": { "$ref": "#/$defs/reference" }
150       }
151     },
152
153     "$defs": {
154       "reference": {
155         "type": "object",
156         "additionalProperties": false,
```

```
      "required": ["id", "url"],
      "properties": {
        "id": { "type": "string" },
        "url": { "type": "string", "format": "uri" }
      }
    },

    "confidence": {
      "description": "Confidence level: number -(0.01.0) or an
         implementation-specific enum/string.",
      "oneOf": [
        { "type": "number", "minimum": 0.0, "maximum": 1.0 },
        { "type": "string" }
      ]
    },

    "evidenceSignal": {
      "oneOf": [
        {
          "type": "string",
          "enum": [
            "in_the_wild_attempts",
            "successful_exploitation",
            "confirmed_compromise",
            "mass_scanning",
            "weaponized_exploit_available"
          ]
        },
        {
          "type": "array",
          "items": {
            "type": "string",
            "enum": [
              "in_the_wild_attempts",
              "successful_exploitation",
              "confirmed_compromise",
              "mass_scanning",
              "weaponized_exploit_available"
            ]
          },
          "minItems": 1,
          "uniqueItems": true
        }
      ]
    },

    "gcveEvidence": {
      "type": "object",
      "additionalProperties": false,
      "properties": {
        "vluuid": {
```

```
            "type": "string",
            "description": "UUID of the Vulnerability-Lookup instance
               where the assertion originated."
          },
          "gna": {
            "type": "integer",
            "minimum": 0,
            "maximum": 65535,
            "description": "GNA ID identifying the origin of the
               assertion."
          },
          "object_uuid": {
            "type": "string",
            "description": "UUID of the assertion associated with this
               evidence in the GCVE ecosystem."
          }
        }
      },

      "evidenceItem": {
        "type": "object",
        "additionalProperties": false,
        "required": ["source"],
        "properties": {
          "type": {
            "type": "string",
            "description": "Origin of the exploitation evidence.",
            "enum": [
              "incident_response",
              "telemetry",
              "honeypot",
              "sinkhole",
              "vendor_report",
              "csirt_report",
              "public_report",
              "research_report",
              "unknown"
            ]
          },
          "signal": {
            "$ref": "#/$defs/evidenceSignal",
            "description": "Nature of the observed exploitation signal (
               string or array of strings)."
          },
          "confidence": { "$ref": "#/$defs/confidence" },
          "source": {
            "type": "string",
            "description": "Logical identifier of the reporting entity or
                data source."
          },
          "details": {
```

```
253             "type": "object",
254             "description": "Structured, free-form metadata describing how
                    the signal was derived (implementation-specific).",
255             "additionalProperties": true
256           },
257           "gcve": {
258             "$ref": "#/$defs/gcveEvidence",
259             "description": "Structured object describing evidence
                   originating from the GCVE ecosystem."
260           }
261         }
262       }
263     }
264 }
```

4 References

- `gcve-eu-kev` scripts - CISA KEV and ENISA CNW EUVD to GCVE BCP-07 Converter: https://github.com/gcve-eu/gcve-eu-kev

5 Acknowledgements

5.1 BCP-07 Coordinators

- Cédric Bonhomme, CIRCL
- Alexandre Dulaunoy, CIRCL

5.2 Contributions

The GCVE initiative gratefully acknowledges the substantial contributions from the following individuals via public review:

- Howard Chu
- Xavier Claude
- Darses
- Jerry Gamblin
- Jay Jacobs
- William Robinet