## 4.18 Vulnerability

**Type Name:** vulnerability

A Vulnerability is a weakness or defect in the requirements, designs, or implementations of the computational logic (e.g., code) found in software and some hardware components (e.g., firmware) that can be directly exploited to negatively impact the confidentiality, integrity, or availability of that system.

CVE is a list of information security vulnerabilities and exposures that provides common names for publicly known problems [[CVE](#kix.a83ojt2ku27w)]. For example, if a piece of malware exploits CVE-2015-12345, a Malware object could be linked to a Vulnerability object that references CVE-2015-12345.

The Vulnerability SDO is primarily used to link to external definitions of vulnerabilities or to describe 0-day vulnerabilities that do not yet have an external definition. Typically, other SDOs assert relationships to Vulnerability objects when a specific vulnerability is targeted and exploited as part of malicious cyber activity. As such, Vulnerability objects can be used as a linkage to the asset management and compliance process.

### 4.18.1 Properties

|  |  |  |
| --- | --- | --- |
| **Required Common Properties** | | |
| **type**, **spec\_version**, **id**, **created**, **modified** | | |
| **Optional Common Properties** | | |
| **created\_by\_ref**, **revoked**, **labels**, **confidence**, **lang**, **external\_references**, **object\_marking\_refs**, **granular\_markings** | | |
| **Not Applicable Common Properties** | | |
| **defanged**, **extensions** | | |
| **Vulnerability Specific Properties** | | |
| **name**, **description** | | |
| **Property Name** | **Type** | **Description** |
| **type** (required) | string | The value of this property MUST be vulnerability. |
| **external\_references**  (optional) | list of type external-reference | A list of external references which refer to non-STIX information. This property **MAY** be used to provide one or more Vulnerability identifiers, such as a CVE ID [[CVE](#kix.a83ojt2ku27w)]. When specifying a CVE ID, the **source\_name** property of the external reference **MUST** be set to cve and the **external\_id** property **MUST** be the exact CVE identifier. |
| **name** (required) | string | A name used to identify the Vulnerability. |
| **description** (optional) | string | A description that provides more details and context about the Vulnerability, potentially including its purpose and its key characteristics. |

### 4.18.2 Relationships

These are the relationships explicitly defined between the Vulnerability object and other STIX Objects. The first section lists the embedded relationships by property name along with their corresponding target. The rest of the table identifies the relationships that can be made from this object type to another object type by way of the Relationship object. The reverse relationships section illustrates the relationships targeting this object type from another object type. They are included here for convenience. For their definitions, please see the "Source" object.

Relationships are not restricted to those listed below. Relationships can be created between any objects using the related-to relationship type or, as with open vocabularies, user-defined names.

|  |  |  |  |
| --- | --- | --- | --- |
| **Embedded Relationships** | | | |
| **created\_by\_ref** | | identifier (of type identity) | |
| **object\_marking\_refs** | | list of type identifier (of type marking-definition) | |
| **Common Relationships** | | | |
| duplicate-of, derived-from, related-to | | | |
| **Source** | **Relationship Type** | **Target** | **Description** |
| — | — | — | — |
| **Reverse Relationships** | | | |
| attack-pattern, campaign, intrusion-set, malware, threat-actor, tool | targets | vulnerability | See forward relationship for definition. |
| malware | exploits | vulnerability | See forward relationship for definition. |
| course-of-action | mitigates, remediates | vulnerability | See forward relationship for definition. |
| infrastructure | has | vulnerability | See forward relationship for definition. |

**​Examples**

{

"type": "vulnerability",

"spec\_version": "2.1",

"id": "vulnerability--0c7b5b88-8ff7-4a4d-aa9d-feb398cd0061",

"created": "2016-05-12T08:17:27.000Z",

"modified": "2016-05-12T08:17:27.000Z",

"created\_by\_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",

"name": "CVE-2016-1234",

"external\_references": [

{

"source\_name": "cve",

"external\_id": "CVE-2016-1234"

}

]

}