Splunk® Common Information Model Add-on Common Information Model Add-on Manual 5.3.2

Vulnerabilities

Generated: 6/06/2024 2:29 pm

Vulnerabilities

The fields in the Vulnerabilities data model describe vulnerability detection data.

Note: A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

Tags used with the Vulnerabilities event datasets

The following tags act as constraints to identify your events as being relevant to this data model. For more information, see How to use these reference tables.

Dataset name	Tag name
Vulnerabilities	report
	vulnerability

Fields for Vulnerabilities event datasets

The following table lists the extracted and calculated fields for the event datasets in the model. Note that it does not include any inherited fields. For more information, see How to use these reference tables.

The key for using the column titled "Notes" or "Abbreviated list of example values" is as follows:

- **Recommended**: Add-on developers make their best effort attempts to map these event fields. If these fields are not populated, then the event is not very useful.
- **Required**: Add-on developers must map these event fields when using the pytest-splunk-addon to test for CIM compatibility. See pytest-splunk-addon documentation.
- **Prescribed values**: Permitted values that can populate the fields, which Splunk is using for a particular purpose. Other valid values exist, but Splunk is not relying on them.
- **Other values**: Other example values that you might see.

Dataset name	Field name	Data type	Description	Notes
Vulnerabilities	`bugtraq`	string	Corresponds to an identifier in the vulnerability database provided by the Security Focus website (searchable at http://www.securityfocus.com/).	
Vulnerabilities	`category`	string	The category of the discovered vulnerability, such as `DoS`. **Note:** This field is a string. Use `category_id` for numeric values. The `category_id` field is optional and thus is not included in the data model.	• recommended • required for pytest-splunk-addon
Vulnerabilities	`cert`	string	Corresponds to an identifier in the vulnerability database provided by the US Computer Emergency Readiness Team (US-CERT, searchable at http://www.kb.cert.org/vuls/).	
Vulnerabilities	`cve`	string	Corresponds to an identifier provided in the Common Vulnerabilities and Exposures index (searchable at http://cve.mitre.org).	• recommended • required for pytest-splunk-addon
Vulnerabilities	`cvss`	number	Numeric indicator of the common vulnerability scoring system.	

Dataset name	Field name	Data type	Description	Notes
				required for pytest-splunk-addon
Vulnerabilities	dest	string	The host with the discovered vulnerability. You can **alias** this from more specific fields, such as dest_host, dest_ip, or dest_name.	• recommended • required for pytest-splunk-addon
Vulnerabilities	dest_bunit	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for these fields when writing add-ons.	
Vulnerabilities	dest_category	string		
Vulnerabilities	dest_priority	string		
Vulnerabilities	dvc	string	The system that discovered the vulnerability. You can **alias** this from more specific fields, such as dvc_host, dvc_ip, or dvc_name.	• recommended • required for pytest-splunk-addon
Vulnerabilities	dvc_bunit	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for these fields when writing add-ons.	
Vulnerabilities	dvc_category	string		
Vulnerabilities	dvc_priority	string		
Vulnerabilities	msft	string	Corresponds to a Microsoft Security Advisory number (http://technet.microsoft.com/en-us/security/advisory/).	
Vulnerabilities	mskb	string	Corresponds to a Microsoft Knowledge Base article number (http://support.microsoft.com/kb/).	
Vulnerabilities	severity	string	The severity of the vulnerability detection event. Specific values are required. Use vendor_severity for the vendor's own human readable strings (such as Good, Bad, and Really Bad). **Note:** This field is a string. Use severity_id for numeric data types.	• recommended • required for pytest-splunk-addon • prescribed values: critical, high, medium, informational, low
Vulnerabilities	severity_id	string	The numeric or vendor specific severity indicator corresponding to the event severity.	
Vulnerabilities	signature	string	The name of the vulnerability detected on the host, such as HPSBMU02785 SSRT100526 rev.2 - HP LoadRunner Running on Windows, Remote Execution of Arbitrary Code, Denial of Service (DoS). **Note:** This field has a string value. Use signature_id for numeric indicators.	• recommended • required for pytest-splunk-addon
Vulnerabilities	signature_id	string	The unique identifier or event code of the event signature.	
Vulnerabilities	tag	string	This automatically generated field is used to access tags from within data models. Do not define extractions for this field when writing add-ons.	
Vulnerabilities	url	string	The URL involved in the discovered vulnerability.	

Dataset name	Field name	Data type	Description	Notes
Vulnerabilities	user	string	The user involved in the discovered vulnerability.	
Vulnerabilities	user_bunit	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for these fields when writing add-ons.	
Vulnerabilities	user_category	string		
Vulnerabilities	user_priority	string		
Vulnerabilities	vendor_product	string	The vendor and product that detected the vulnerability. This field can be automatically populated by vendor and product fields in your data.	recommended
Vulnerabilities	xref	string	A cross-reference identifier associated with the vulnerability. In most cases, the xref field contains both the short name of the database being cross-referenced and the unique identifier used in the external database.	