NVD Data Map Overview

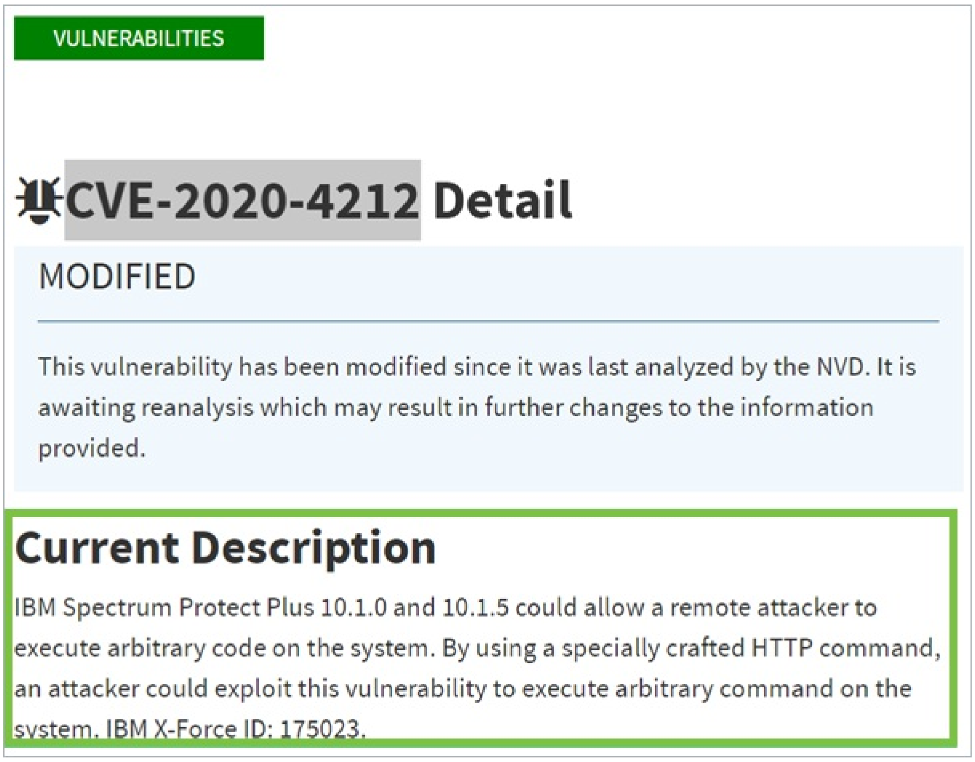
When importing a .json file into RiskVision, the NVD Connector will populate different fields depending on which data feed the file comes from.

When Importing CVE Files

RiskVision will capture the following from the NVD website:

Description

The **Current Description** and **Analysis Description** will be uploaded to the **Description** field of a vulnerability's **General** tab.



CVE-2020-4212 Detail

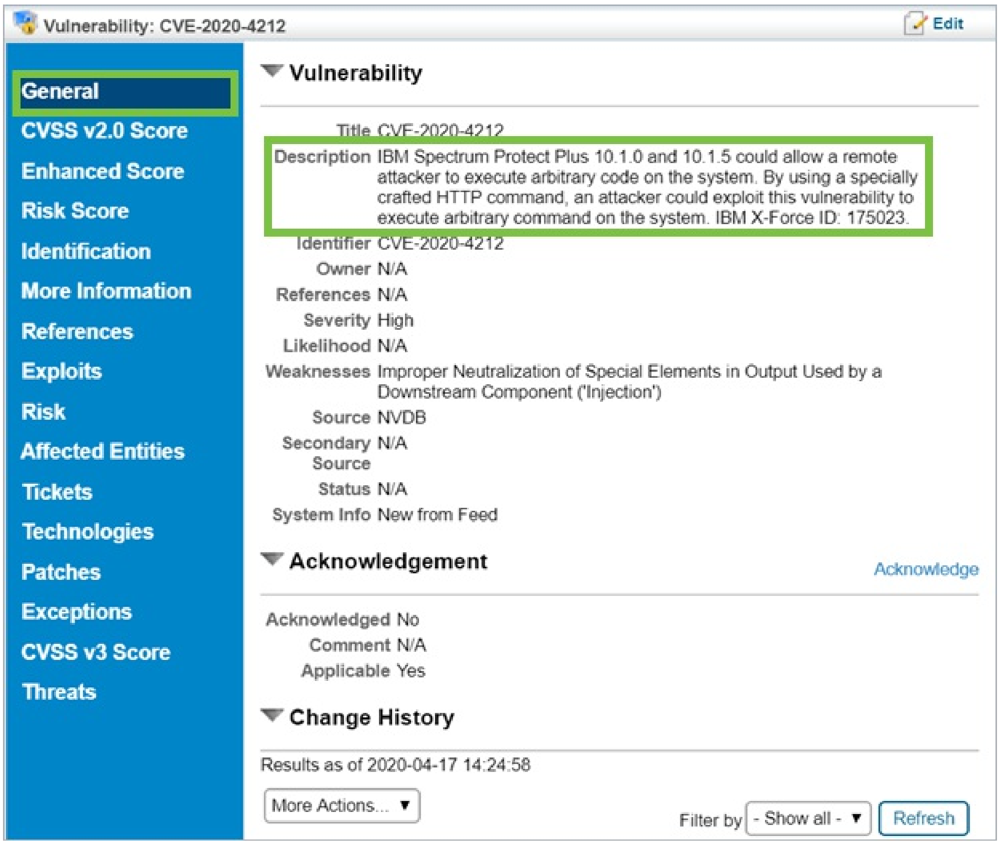
MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Current Description

IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175023.

The Current Description of a CVE file.



Vulnerability

Title CVE-2020-4212
Description IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175023.
Identifier CVE-2020-4212
Owner N/A
References N/A
Severity High
Likelihood N/A
Weaknesses Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')
Source NVDB
Secondary Source N/A
Status N/A
System Info New from Feed

Acknowledgement

Acknowledged No
Comment N/A
Applicable Yes

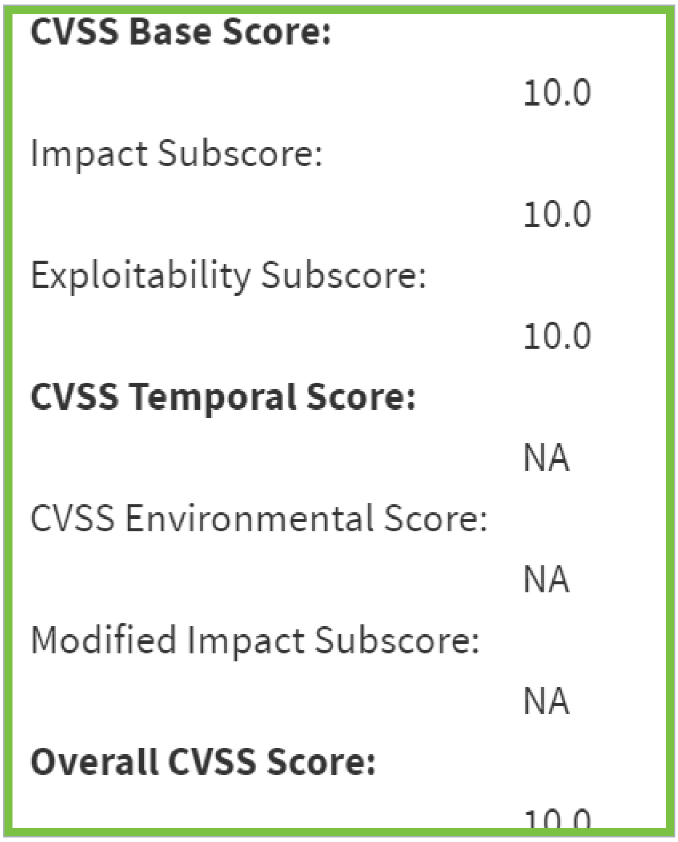
Change History

Results as of 2020-04-17 14:24:58

The CVE's description captured by the Description field in RiskVision.

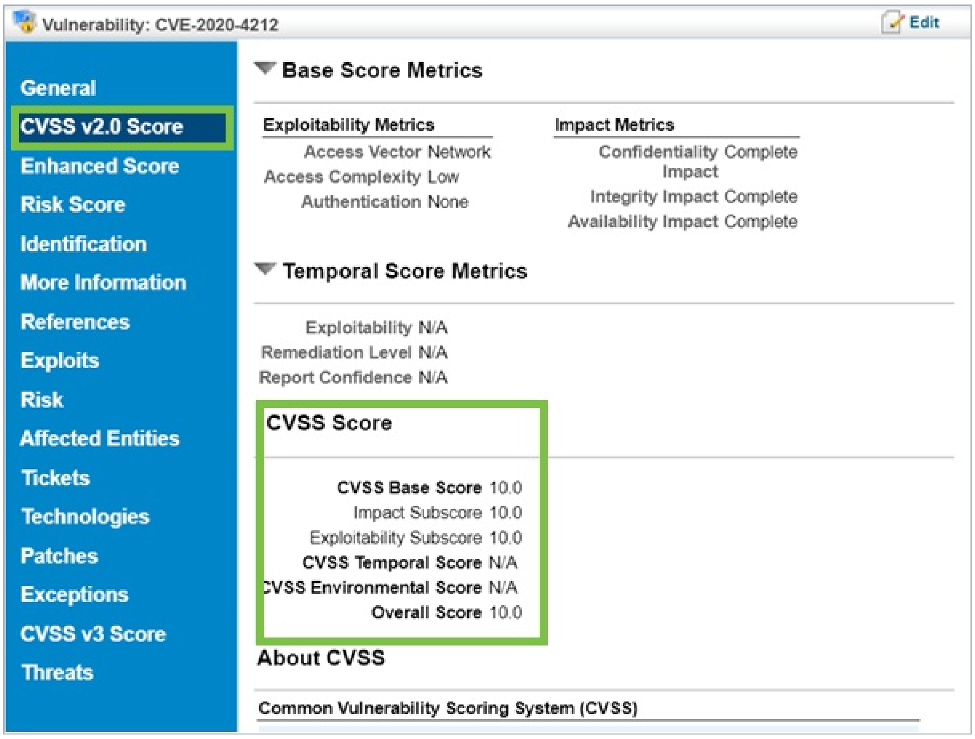
Severity

The vulnerability's **CVSS v2.0 Score** tab will capture all scores from the file's**CVSS Score** section.



CVSS Base Score:
10.0
Impact Subscore:
10.0
Exploitability Subscore:
10.0
CVSS Temporal Score:
NA
CVSS Environmental Score:
NA
Modified Impact Subscore:
NA
Overall CVSS Score:
10.0

The CVSS Score section of a CVE file.



Vulnerability: CVE-2020-4212

Base Score Metrics

Exploitability Metrics		Impact Metrics	
Access Vector	Network	Confidentiality Impact	Complete
Access Complexity	Low	Integrity Impact	Complete
Authentication	None	Availability Impact	Complete

Temporal Score Metrics

Exploitability	N/A
Remediation Level	N/A
Report Confidence	N/A

CVSS Score

CVSS Base Score	10.0
Impact Subscore	10.0
Exploitability Subscore	10.0
CVSS Temporal Score	N/A
CVSS Environmental Score	N/A
Overall Score	10.0

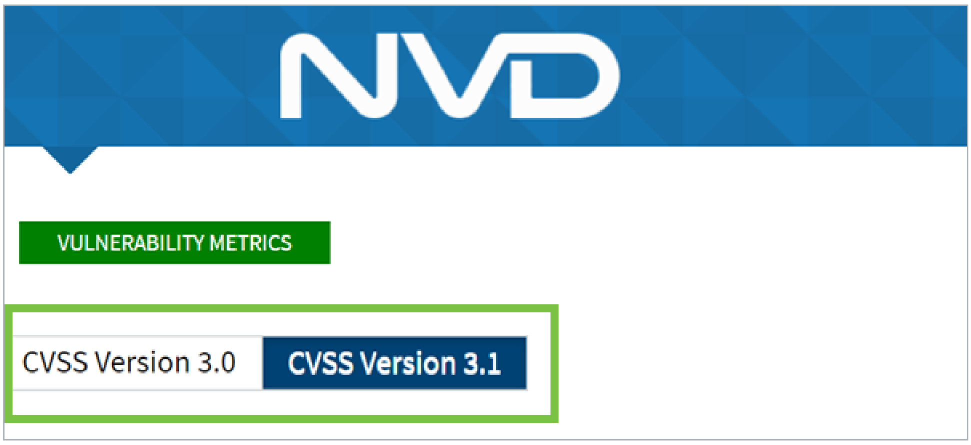
About CVSS

Common Vulnerability Scoring System (CVSS)

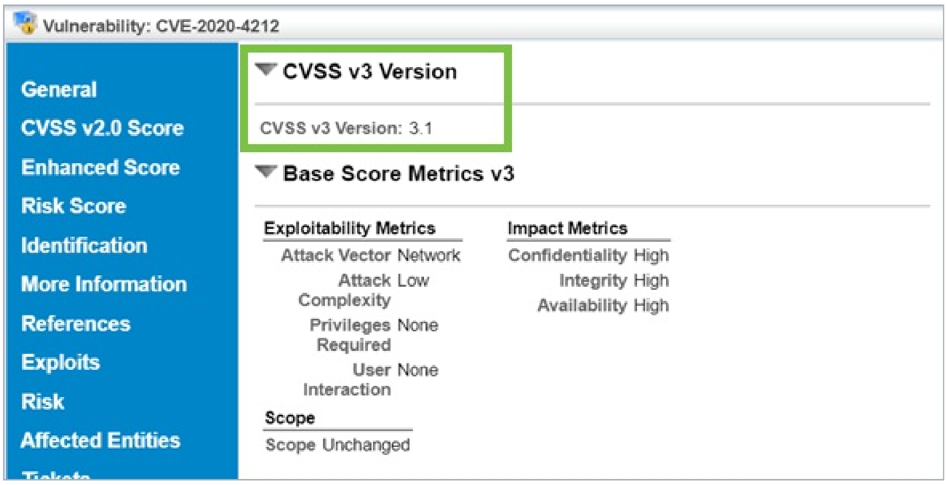
The CVE's severity scores captured by the CVSS Score field in RiskVision.

The **CVSS v3 Score** tab will capture all fields and values in the following sections of the .json file:

- **CVSS v3 Version**



The CVSS version of a CVE file.


Vulnerability: CVE-2020-4212

CVSS v3 Version

CVSS v3 Version: 3.1

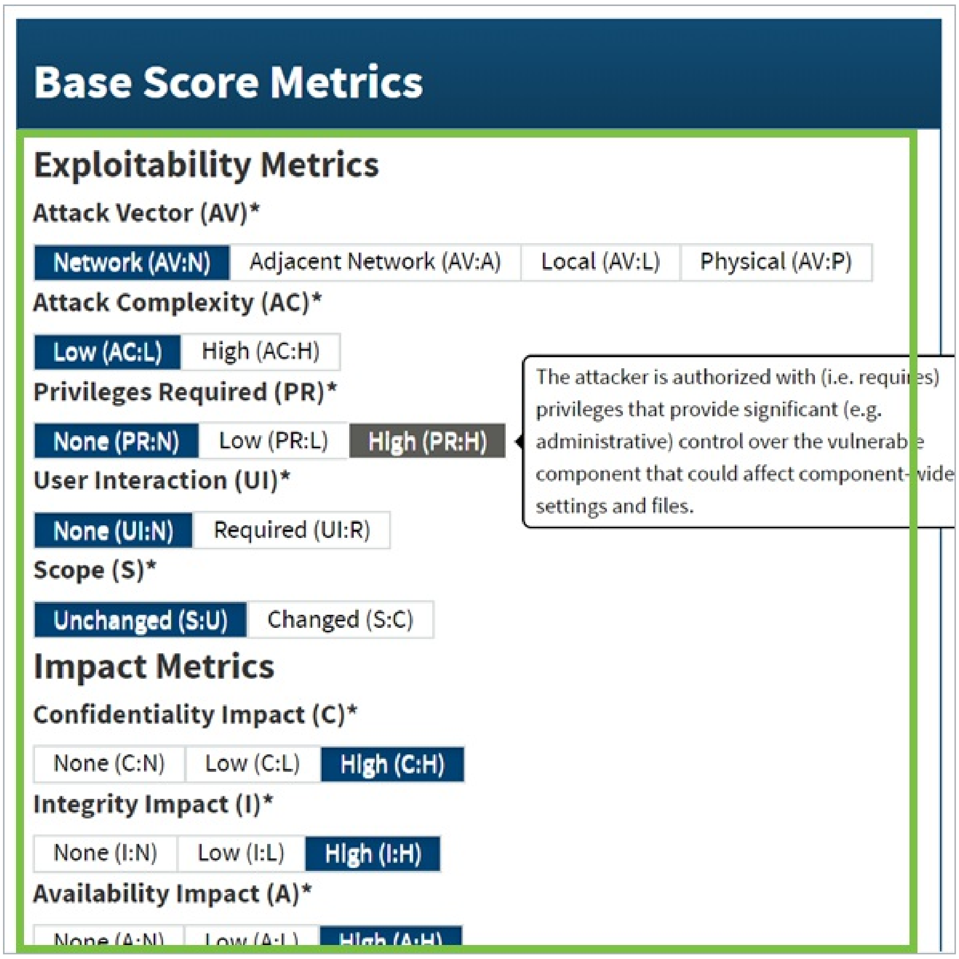
Base Score Metrics v3

Exploitability Metrics		Impact Metrics	
Attack Vector	Network	Confidentiality	High
Attack Complexity	Low	Integrity	High
Privileges Required	None	Availability	High
User Interaction	None		

Scope	
Scope	Unchanged

The CVE's CVSS v3 Version captured in RiskVision.

- Base Score Metrics v3



Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L) | High (AC:H)

Privileges Required (PR)*

None (PR:N) | Low (PR:L) | High (PR:H)

The attacker is authorized with (i.e. requires) privileges that provide significant (e.g. administrative) control over the vulnerable component that could affect component-wide settings and files.

User Interaction (UI)*

None (UI:N) | Required (UI:R)

Scope (S)*

Unchanged (S:U) | Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N) | Low (C:L) | High (C:H)

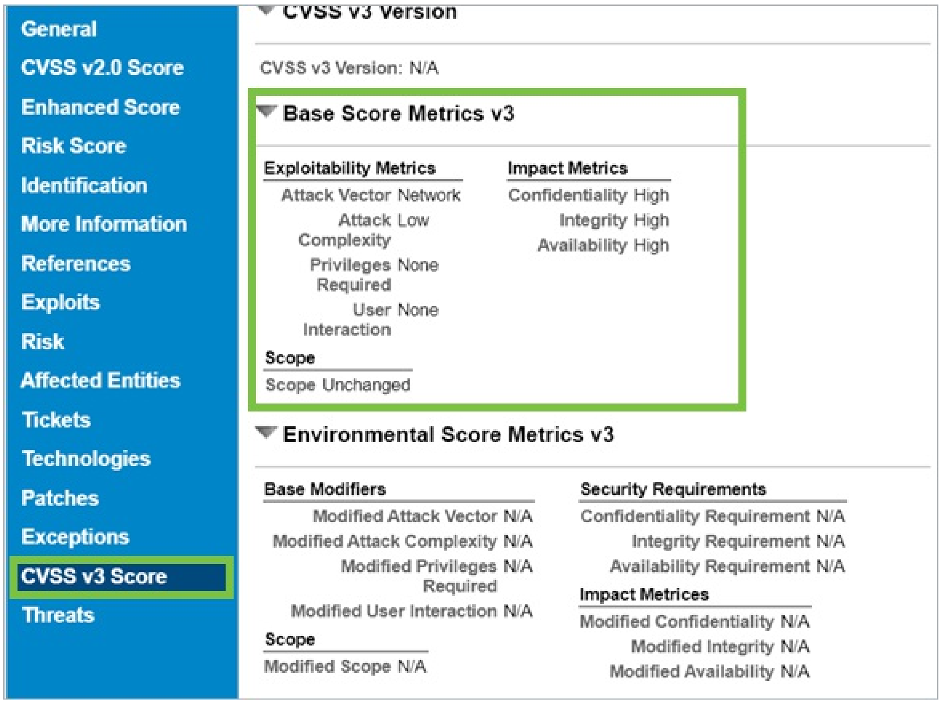
Integrity Impact (I)*

None (I:N) | Low (I:L) | High (I:H)

Availability Impact (A)*

None (A:N) | Low (A:L) | High (A:H)

The Base Score Metrics of a CVE file.



CVSS v3 Version

CVSS v3 Version: N/A

Base Score Metrics v3

Exploitability Metrics	
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None

Impact Metrics	
Confidentiality	High
Integrity	High
Availability	High

Scope	
Scope	Unchanged

Environmental Score Metrics v3

Base Modifiers	
Modified Attack Vector	N/A
Modified Attack Complexity	N/A
Modified Privileges Required	N/A
Modified User Interaction	N/A

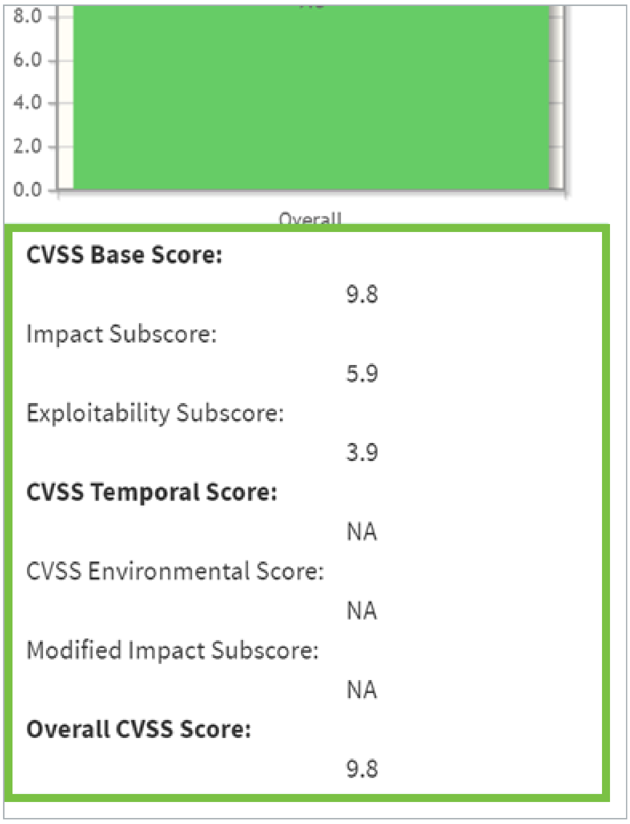
Scope	
Modified Scope	N/A

Security Requirements	
Confidentiality Requirement	N/A
Integrity Requirement	N/A
Availability Requirement	N/A

Impact Metrices	
Modified Confidentiality	N/A
Modified Integrity	N/A
Modified Availability	N/A

The CVE's Base Score Metrics captured in RiskVision.

- CVSS v3 Score



CVSS Base Score: 9.8

Impact Subscore: 5.9

Exploitability Subscore: 3.9

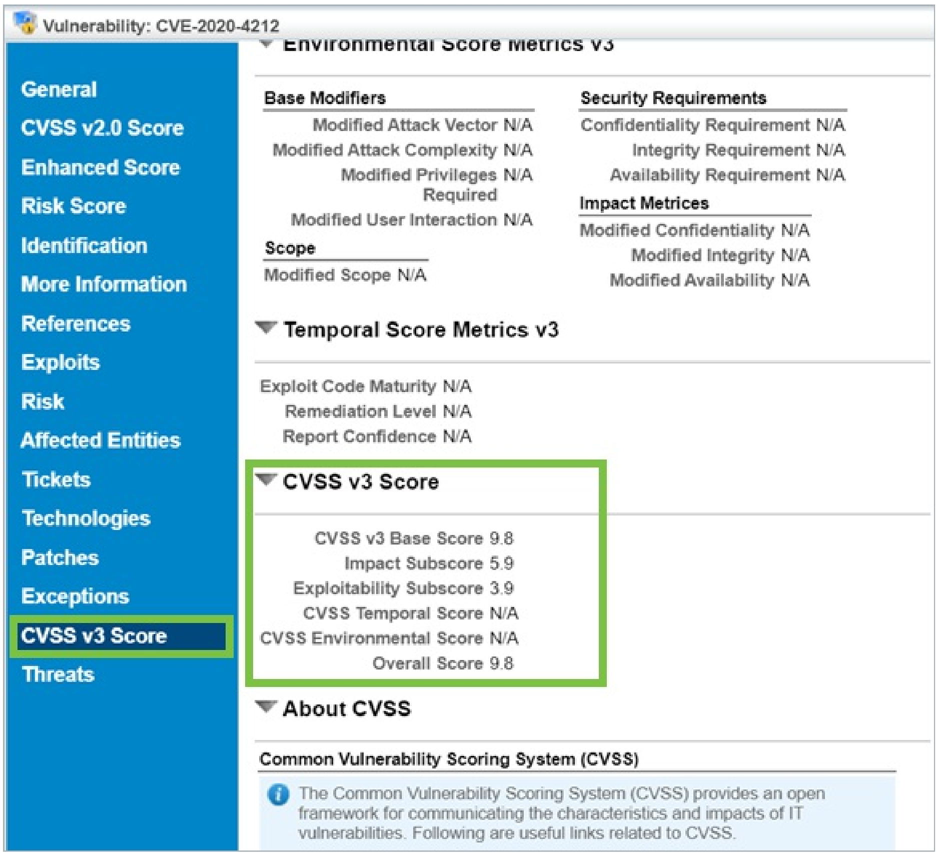
CVSS Temporal Score: NA

CVSS Environmental Score: NA

Modified Impact Subscore: NA

Overall CVSS Score: 9.8

The CVSS V3 Scores of a CVE file.



Environmental Score Metrics v3

Base Modifiers

Modified Attack Vector N/A
Modified Attack Complexity N/A
Modified Privileges Required N/A
Modified User Interaction N/A

Scope

Modified Scope N/A

Security Requirements

Confidentiality Requirement N/A
Integrity Requirement N/A
Availability Requirement N/A

Impact Metrices

Modified Confidentiality N/A
Modified Integrity N/A
Modified Availability N/A

Temporal Score Metrics v3

Exploit Code Maturity N/A
Remediation Level N/A
Report Confidence N/A

CVSS v3 Score

CVSS v3 Base Score 9.8
Impact Subscore 5.9
Exploitability Subscore 3.9
CVSS Temporal Score N/A
CVSS Environmental Score N/A
Overall Score 9.8

About CVSS

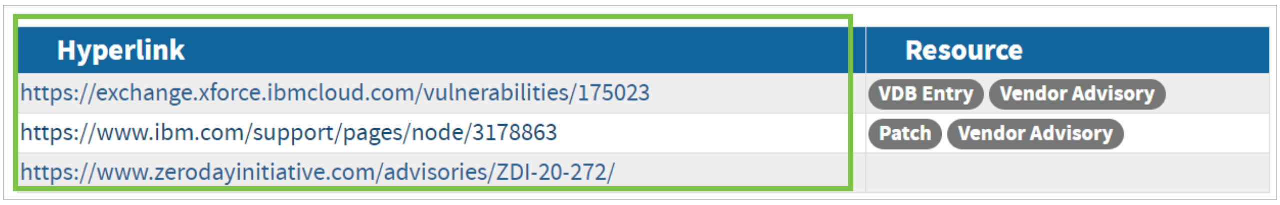
Common Vulnerability Scoring System (CVSS)

The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. Following are useful links related to CVSS.

The CVE's CVSS v3 Score captured in RiskVision.

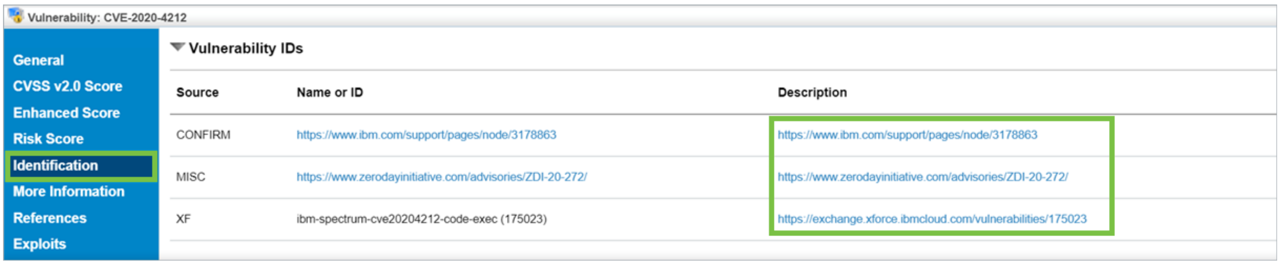
Hyperlinks

All related hyperlinks will be captured in the **Description** field of the vulnerability's **Identification** tab.



Hyperlink	Resource
https://exchange.xforce.ibmcloud.com/vulnerabilities/175023	VDB Entry Vendor Advisory
https://www.ibm.com/support/pages/node/3178863	Patch Vendor Advisory
https://www.zerodayinitiative.com/advisories/ZDI-20-272/	

The Hyperlink section of a CVE file.

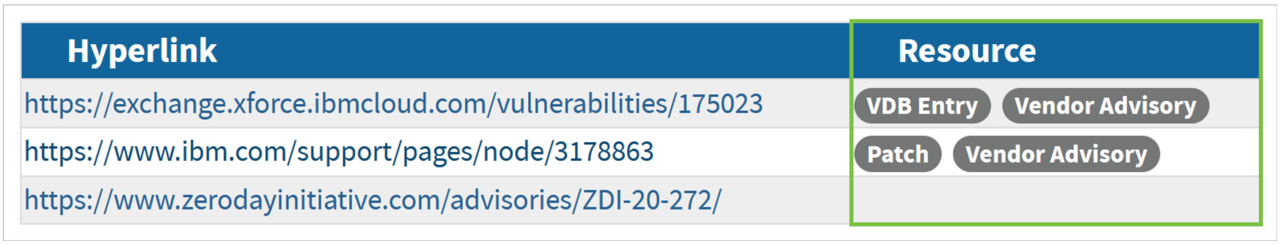


Source	Name or ID	Description
CONFIRM	https://www.ibm.com/support/pages/node/3178863	https://www.ibm.com/support/pages/node/3178863
MISC	https://www.zerodayinitiative.com/advisories/ZDI-20-272/	https://www.zerodayinitiative.com/advisories/ZDI-20-272/
XF	ibm-spectrum-cve20204212-code-exec (175023)	https://exchange.xforce.ibmcloud.com/vulnerabilities/175023

The CVE's hyperlinks captured in the Description field in RiskVision.

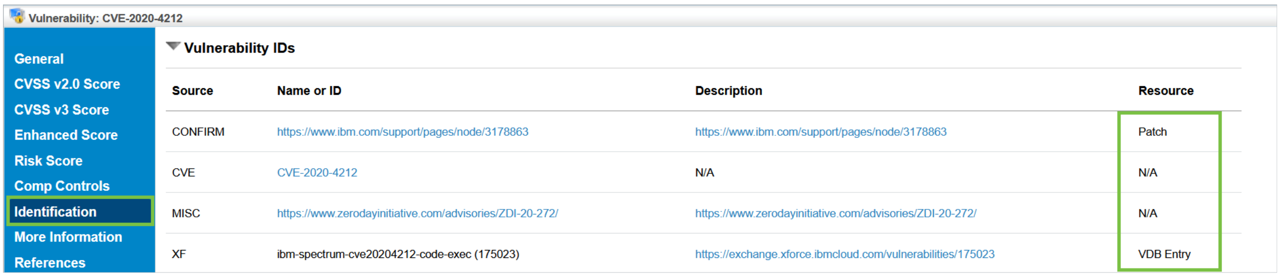
Resources

All related resources will be captured in the **Resource** field of the vulnerabilities **Identification** tab.



Hyperlink	Resource
https://exchange.xforce.ibmcloud.com/vulnerabilities/175023	VDB Entry Vendor Advisory
https://www.ibm.com/support/pages/node/3178863	Patch Vendor Advisory
https://www.zerodayinitiative.com/advisories/ZDI-20-272/	

The Resource section of a CVE file.

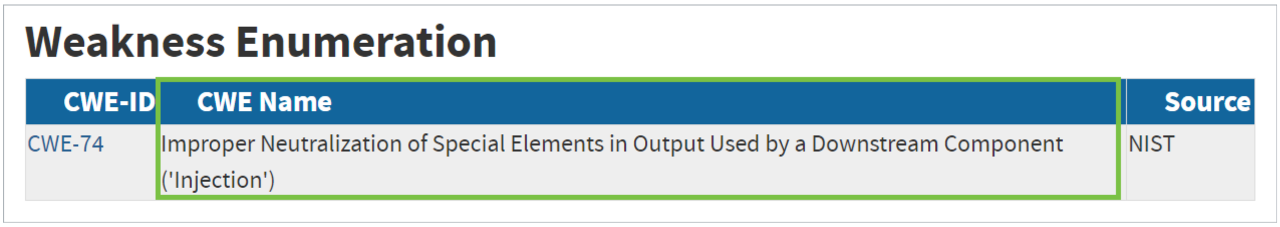


Source	Name or ID	Description	Resource
CONFIRM	https://www.ibm.com/support/pages/node/3178863	https://www.ibm.com/support/pages/node/3178863	Patch
CVE	CVE-2020-4212	N/A	N/A
MISC	https://www.zerodayinitiative.com/advisories/ZDI-20-272/	https://www.zerodayinitiative.com/advisories/ZDI-20-272/	N/A
XF	ibm-spectrum-cve20204212-code-exec (175023)	https://exchange.xforce.ibmcloud.com/vulnerabilities/175023	VDB Entry

The CVE's resources captured in the Resource field in RiskVision.

Weakness Enumeration

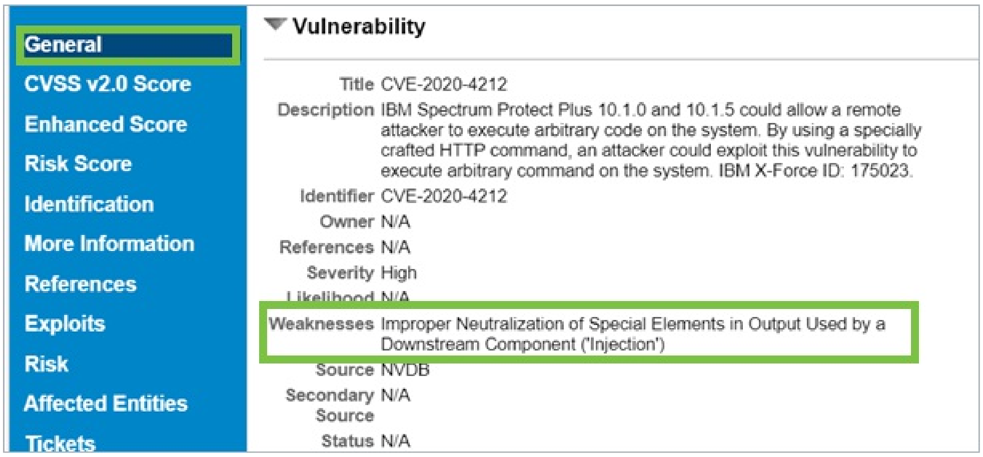
The .json file's **CWE Name** will be captured in the **Weaknesses** field of the vulnerability's **General** tab. The **CWE-ID** and **Source** will not be captured.



Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-74	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	NIST

The CWE Name of a weakness in a CWE file.

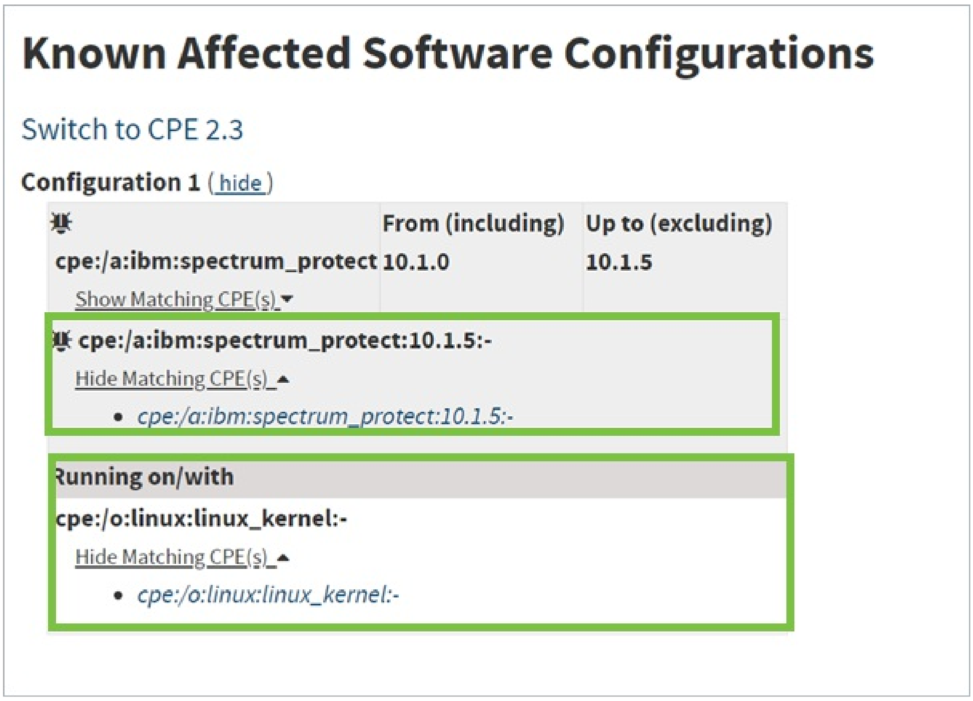


Title	CVE-2020-4212
Description	IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175023.
Identifier	CVE-2020-4212
Owner	N/A
References	N/A
Severity	High
Likelihood	N/A
Weaknesses	Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')
Source	NVDB
Secondary Source	N/A
Status	N/A

The CWE Name captured in the Weaknesses field in RiskVision.

Known Affected Software Configurations

These will be captured in the vulnerability's **Technologies** tab.



Known Affected Software Configurations

Switch to CPE 2.3

Configuration 1 (hide)

	From (including)	Up to (excluding)
cpe:/a:ibm:spectrum_protect Show Matching CPE(s)	10.1.0	10.1.5
cpe:/a:ibm:spectrum_protect:10.1.5:- Hide Matching CPE(s) • cpe:/a:ibm:spectrum_protect:10.1.5:-		

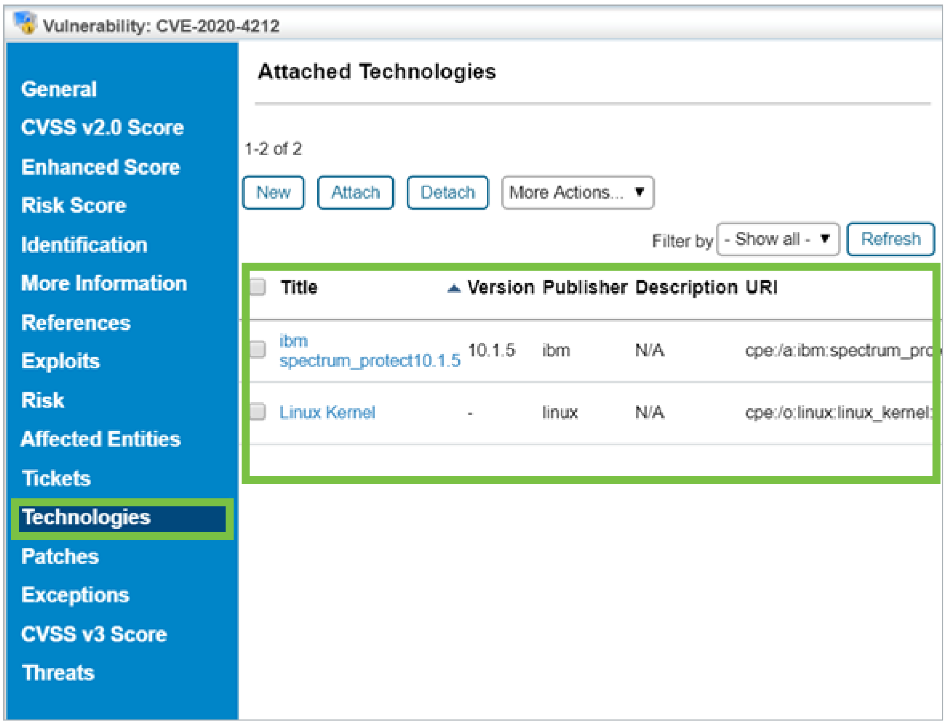
Running on/with

cpe:/o:linux:linux_kernel:-

Hide Matching CPE(s)

- cpe:/o:linux:linux_kernel:-

The Known Affected Software Configurations of a CVE file.



Attached Technologies

1-2 of 2

□	Title	▲ Version	Publisher	Description	URI
□	ibm spectrum_protect10.1.5	10.1.5	ibm	N/A	cpe:/a:ibm:spectrum_pro
□	Linux Kernel	-	linux	N/A	cpe:/o:linux:linux_kernel:

The CVE file's Known Affected Software Configurations captured in RiskVision.

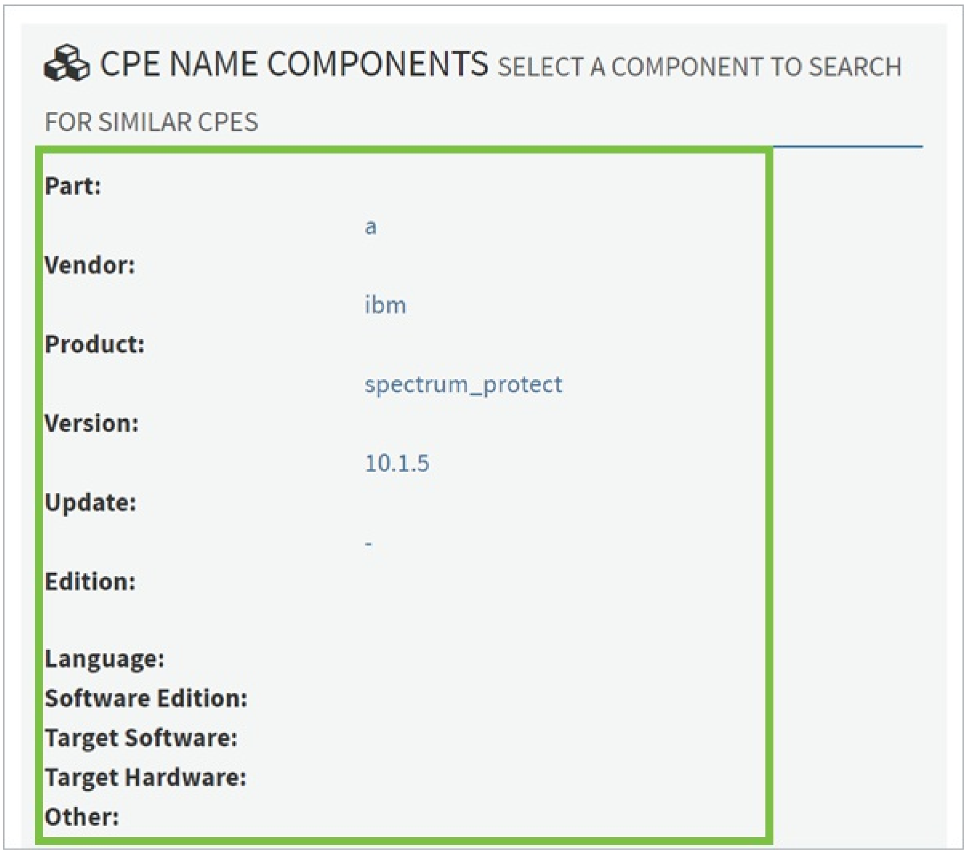
When Importing CPE Files

RiskVision will capture the following from the NVD website:

CPE Names

RiskVision can only import names from version 2.2 of CPE. The following components will be captured by the**General** tab of a technology:

- Part
- Vendor
- Product
- Cloud-init
- Version
- Update
- Edition
- Language



CPE NAME COMPONENTS SELECT A COMPONENT TO SEARCH FOR SIMILAR CPES

Part: a

Vendor: ibm

Product: spectrum_protect

Version: 10.1.5

Update: -

Edition:

Language:

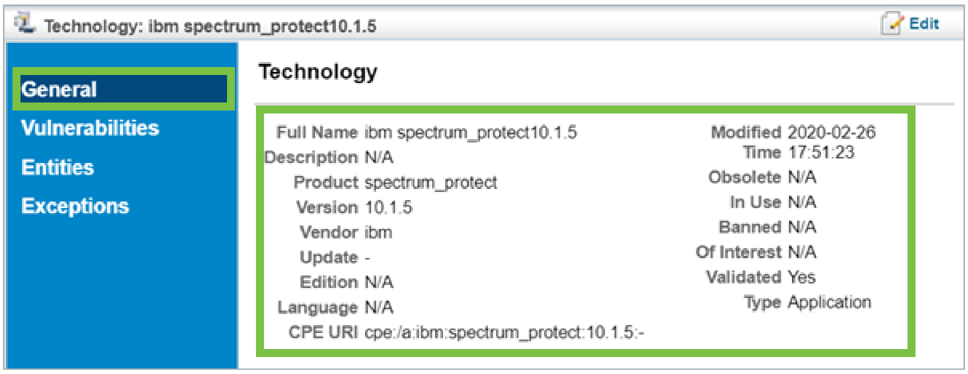
Software Edition:

Target Software:

Target Hardware:

Other:

The Name Components of a CPE file.



Technology: ibm spectrum_protect10.1.5

Technology

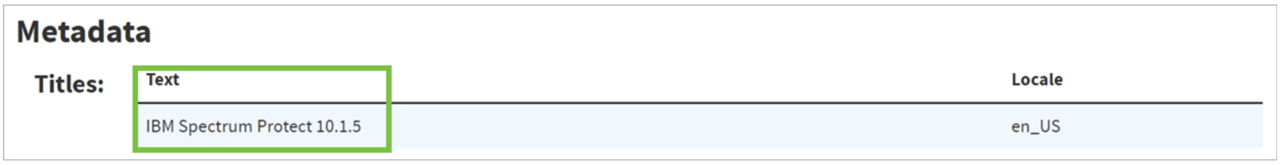
Full Name ibm spectrum_protect10.1.5
Description N/A
Product spectrum_protect
Version 10.1.5
Vendor ibm
Update -
Edition N/A
Language N/A
CPE URI cpe:/a:ibm:spectrum_protect:10.1.5:-

Modified 2020-02-26
Time 17:51:23
Obsolete N/A
In Use N/A
Banned N/A
Of Interest N/A
Validated Yes
Type Application

The CPE name components captured in RiskVision.

Metadata

The **Text** title will be captured by the**Full Name** field in a technology's **General** tab, but the **Locale** title will not.

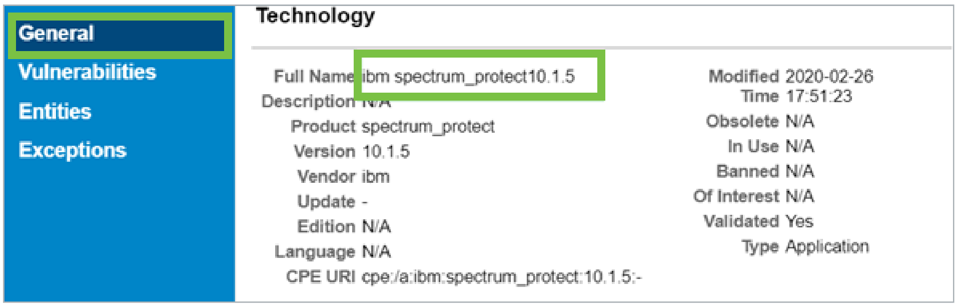


Metadata

Titles:

Text	Locale
IBM Spectrum Protect 10.1.5	en_US

The Text title in a CPE file.



Technology

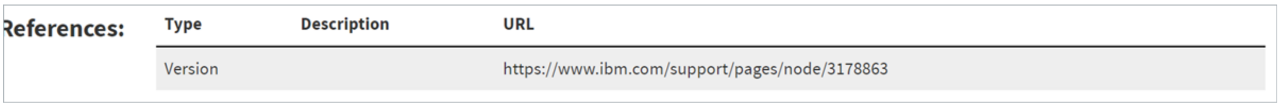
Full Name ibm spectrum_protect10.1.5
Description N/A
Product spectrum_protect
Version 10.1.5
Vendor ibm
Update -
Edition N/A
Language N/A
CPE URI cpe:/a:ibm:spectrum_protect:10.1.5:-

Modified 2020-02-26
Time 17:51:23
Obsolete N/A
In Use N/A
Banned N/A
Of Interest N/A
Validated Yes
Type Application

The CPE's Text title captured by the Full Name field in RiskVision.

References

This section is not captured as they contain **Change Log** data.



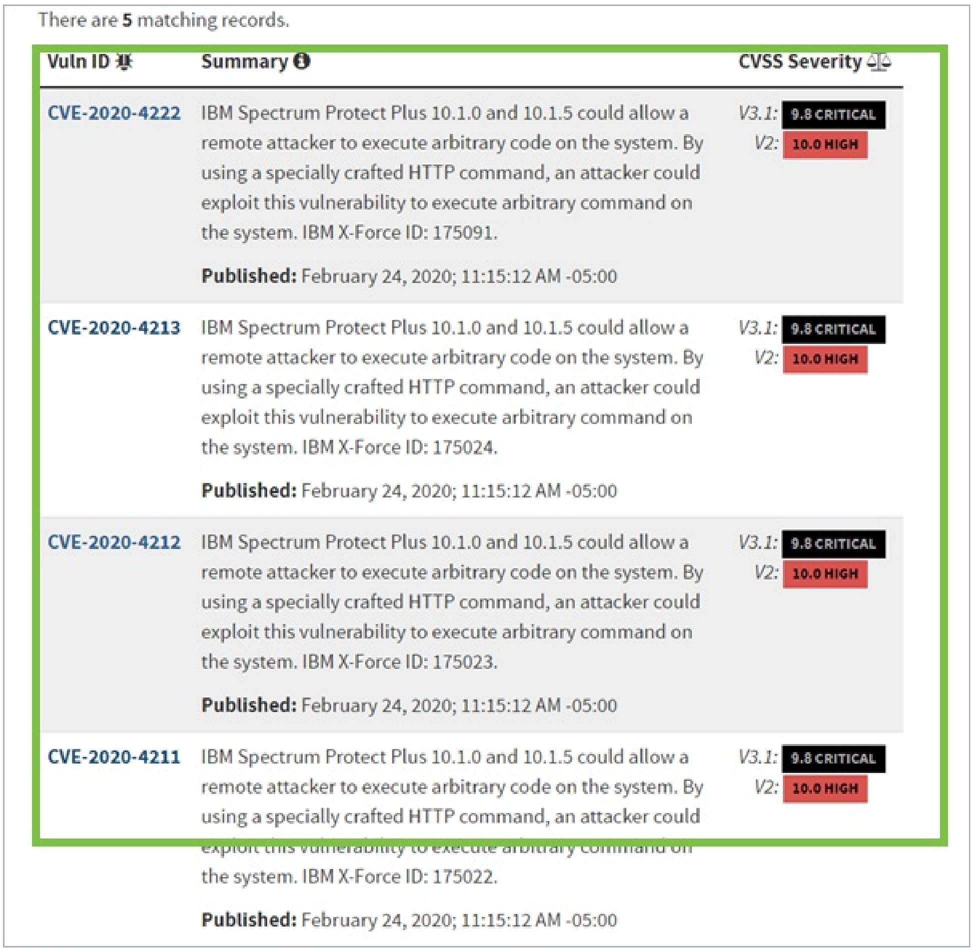
References:

Type	Description	URL
Version		https://www.ibm.com/support/pages/node/3178863

The References section of a CPE file.

CPE Usage

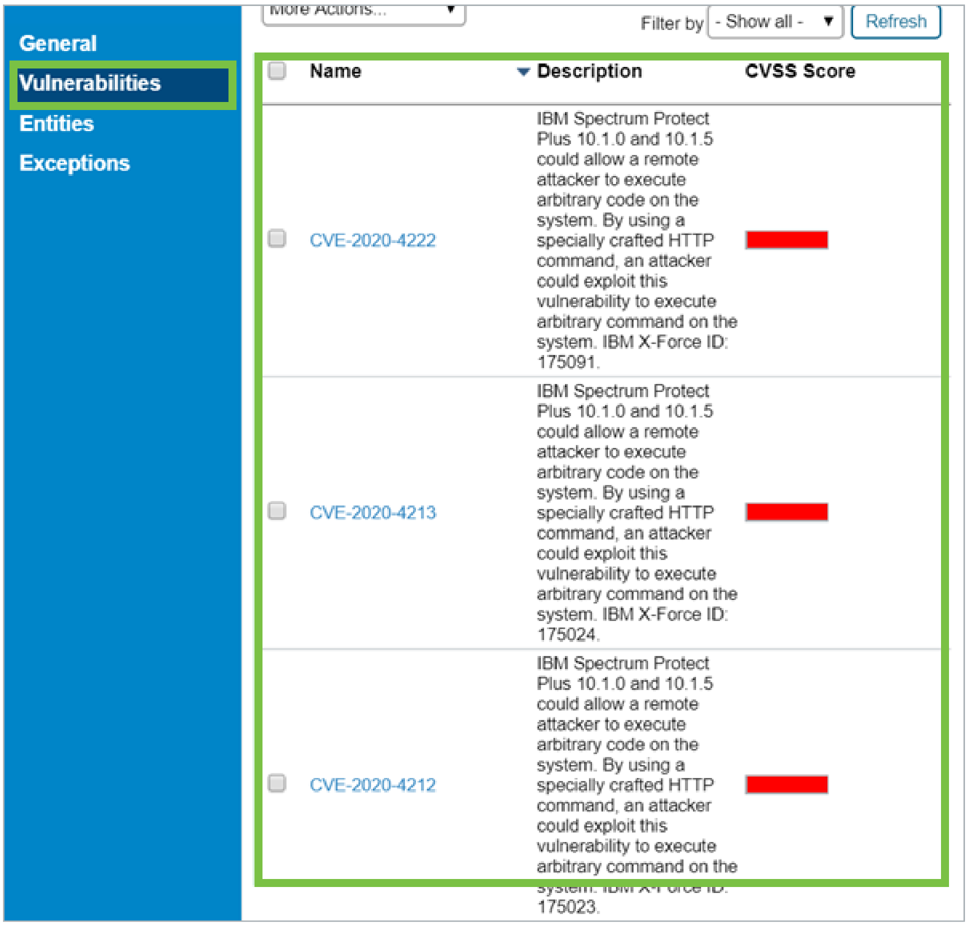
View and Associated vulnerabilities will be captured in RiskVision's **Vulnerabilities** tab for threats and technologies.



There are **5** matching records.

Vuln ID	Summary	CVSS Severity
CVE-2020-4222	IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175091. **Published:** February 24, 2020; 11:15:12 AM -05:00	V3.1: 9.8 CRITICAL V2: 10.0 HIGH
CVE-2020-4213	IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175024. **Published:** February 24, 2020; 11:15:12 AM -05:00	V3.1: 9.8 CRITICAL V2: 10.0 HIGH
CVE-2020-4212	IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175023. **Published:** February 24, 2020; 11:15:12 AM -05:00	V3.1: 9.8 CRITICAL V2: 10.0 HIGH
CVE-2020-4211	IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175022. **Published:** February 24, 2020; 11:15:12 AM -05:00	V3.1: 9.8 CRITICAL V2: 10.0 HIGH

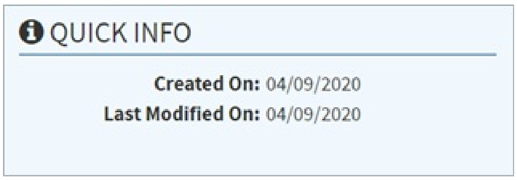
Vulnerabilities in a CPE file.



☐	Name	Description	CVSS Score
☐	CVE-2020-4222	IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175091.	🟥
☐	CVE-2020-4213	IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175024.	🟥
☐	CVE-2020-4212	IBM Spectrum Protect Plus 10.1.0 and 10.1.5 could allow a remote attacker to execute arbitrary code on the system. By using a specially crafted HTTP command, an attacker could exploit this vulnerability to execute arbitrary command on the system. IBM X-Force ID: 175023.	🟥

The CPE's Vulnerabilities captured in RiskVision.

The connector will not capture the file's quick info such as published dates and last modified dates.

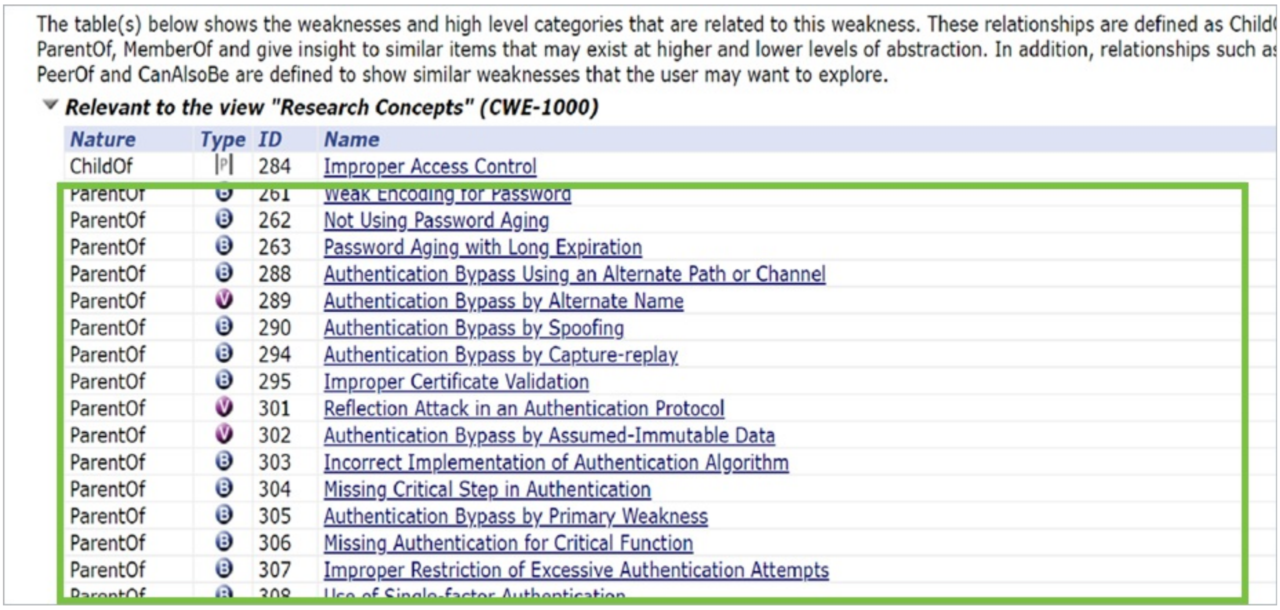

QUICK INFO

Created On: 04/09/2020
Last Modified On: 04/09/2020

The Quick Info of a CPE file.

When Importing CWE Files

While the NVD connector will import files from the CWE datafeed, it will import data from adifferent site than the NVD site. As of now, RiskVision will only capture **Parent Of** information from CWE files in the **General** tab of a weakness.

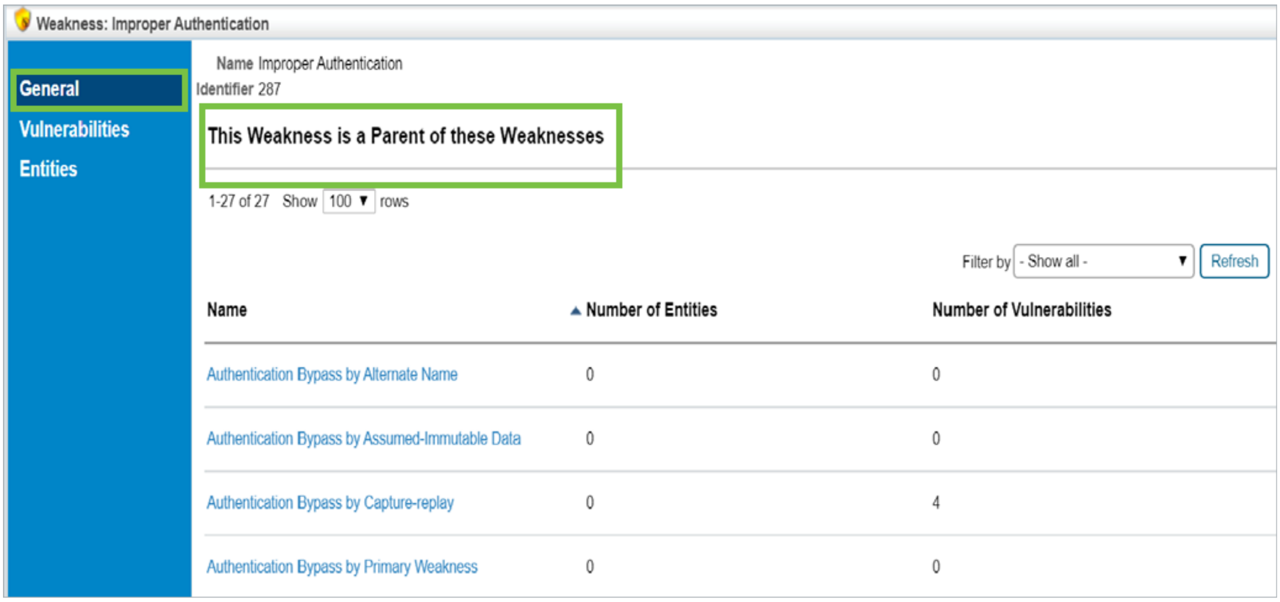


The table(s) below shows the weaknesses and high level categories that are related to this weakness. These relationships are defined as Child ParentOf, MemberOf and give insight to similar items that may exist at higher and lower levels of abstraction. In addition, relationships such as PeerOf and CanAlsoBe are defined to show similar weaknesses that the user may want to explore.

Relevant to the view "Research Concepts" (CWE-1000)

Nature	Type	ID	Name
ChildOf	P	284	Improper Access Control
ParentOf	B	261	Weak Encoding for Password
ParentOf	B	262	Not Using Password Aging
ParentOf	B	263	Password Aging with Long Expiration
ParentOf	B	288	Authentication Bypass Using an Alternate Path or Channel
ParentOf	V	289	Authentication Bypass by Alternate Name
ParentOf	B	290	Authentication Bypass by Spoofing
ParentOf	B	294	Authentication Bypass by Capture-replay
ParentOf	B	295	Improper Certificate Validation
ParentOf	V	301	Reflection Attack in an Authentication Protocol
ParentOf	V	302	Authentication Bypass by Assumed-Immutable Data
ParentOf	B	303	Incorrect Implementation of Authentication Algorithm
ParentOf	B	304	Missing Critical Step in Authentication
ParentOf	B	305	Authentication Bypass by Primary Weakness
ParentOf	B	306	Missing Authentication for Critical Function
ParentOf	B	307	Improper Restriction of Excessive Authentication Attempts
ParentOf	B	308	Use of Single-factor Authentication

The Parent Of information in a CWE file.



Weakness: Improper Authentication

Name Improper Authentication
Identifier 287

This Weakness is a Parent of these Weaknesses

1-27 of 27 Show 100 ▼ rows

Filter by - Show all - ▼ Refresh

Name	▲ Number of Entities	Number of Vulnerabilities
Authentication Bypass by Alternate Name	0	0
Authentication Bypass by Assumed-Immutable Data	0	0
Authentication Bypass by Capture-replay	0	4
Authentication Bypass by Primary Weakness	0	0

The Parent Of information from a CWE file captured in RiskVision.