Calculate a Vulnerability Risk Factor

The Vulnerability Risk Factor estimates the likelihood of a vulnerability instance being exploited on an entity. There are two mutually exclusive ways to set a vulnerability risk factor:

1. CVSS v2.0 score
2. Enhanced score

Your administrator chooses whether to use the CVSS v2.0 score or the Enhanced score as the Vulnerability Risk Factor. The CVSS v2.0 score is more difficult to use. Although it's possible to change your selection, we recommend you don't change methods.

If you use the CVSS v2.0 score, it will be used as the Vulnerability Risk Factor, and will be multiplied by the Entity Criticality Factor to determine the Vulnerability Instance Risk Score. The CVSS score works on a 0-10 scale.

The CVSS score will come from the scanner that reports the vulnerability. In contrast, the Enhanced score takes into account the following variables:

1. CVSS v2.0 Confidentiality Impact Vector.
   The possible values are:
   - None: 0.
   - Partial: 1
   - Complete: 2
2. CVSS v2.0 Integrity Impact Vector.
   The possible values are:
   - None: 0.
   - Partial: 1
   - Complete: 2
3. CVSS v2.0 Availability Impact Vector.
   The possible values are:
   - None: 0.
   - Partial: 1
   - Complete: 2
4. CVSS v2.0 Access Complexity.
   The possible values are:
   - Low: 1
   - Medium: 3
   - High: 5
5. CVSS v2.0 Access Vector.
   The possible values are:
   - Local: 1
   - Adjacent Network: 3
   - Network: 5.
6. CVSS v2.0 Authentication Vector.
   The possible values are:
   - Multiple: 1

    - Single: 3
    - None: 5

7. The number of days a vulnerability has been open: Calculated as the difference between the current date and the date the CVE vulnerability was published. This number is significant because the longer a vulnerability has been open, the more likely it is to be exploited.
8. Exploit Factor: Whether there is a known exploit for the vulnerability, and its exploit type. When more than one exploit maps to a vulnerability, the equation will select the exploit with the highest Exploit Factor. The possible values are:
    - Local: Local access to the computer in question is required to exploit the vulnerability. Value = .6.
    - Remote: The exploit can be conducted across a network. Value = 1.
    - Shellcode: Value = .6
    - WebApp: A web application. Value = 1
    - DOS: Results in a Denial of Service attack. Value = .5
    - No matching exploit: Value = .25

The formula for the Enhanced Vulnerability Risk Score is:

```
Enhanced Score=(Numerator/Denominator) X Threat factor X Exploit Factor X SQ
                                       RT(Days
                                       Known*)
```

where:

```
Numerator = Factorial(Confidentiality + Integrity + Availability)
```

and

```
Denominator = Square(Access Complexity + Authentication + Access Vector)
```

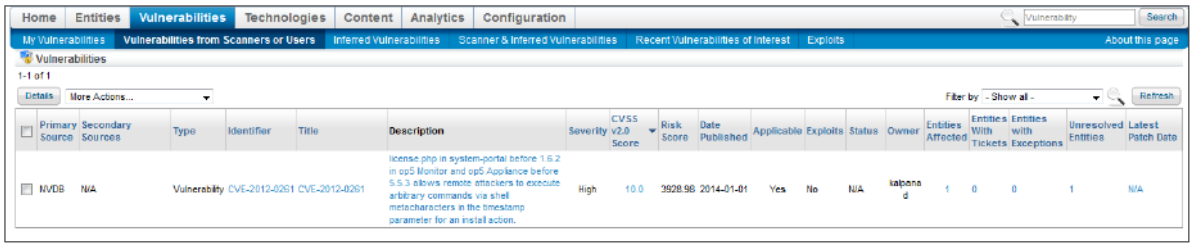
- Days Known is capped at 730 days, which equates to 2 years. The above data shows the actual number of days the vulnerability has been known, but the formula does not allow the Days Known value to exceed 730.
- If there is a threat that matches the vulnerability, the default value is 2. If there is no matching threat, then the default value is 1.

The Enhanced Score is calculated for each CVE that maps to a scanner-reported vulnerability. For example, McAfee Vulnerability Manager ID 140978, Red Hat Enterprise Linux RHSA-2015-2506 Update Is Not Installed, has 19 CVEs that map to it. An Enhanced Score will be calculated for each of the 19 CVEs that map to it, then the Enhanced Scores for these 19 CVEs that map to the scanner-reported vulnerability will be summed up to create the total Enhanced Score for the scanner-reported vulnerability.

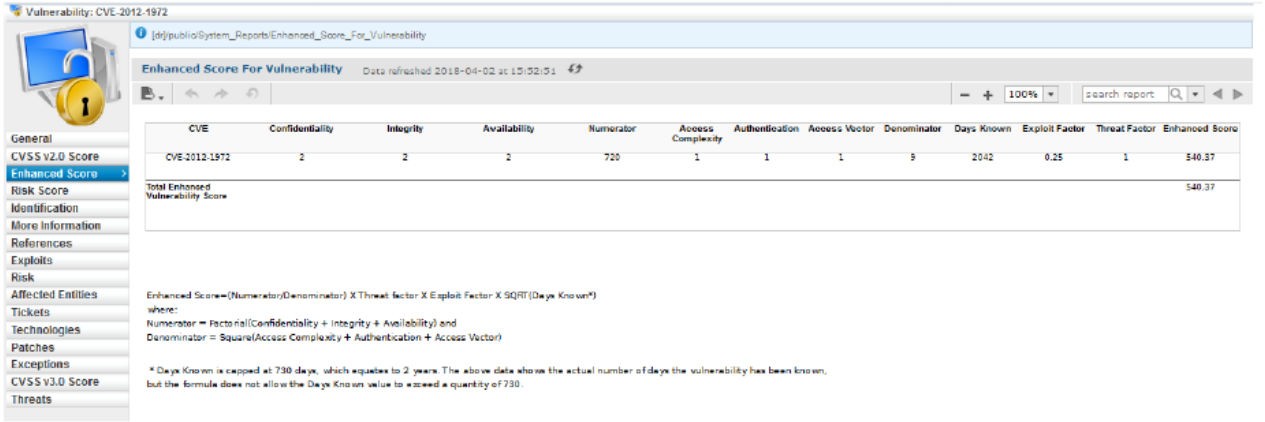
Placement of the Vulnerability Risk Score in the RiskVision UI

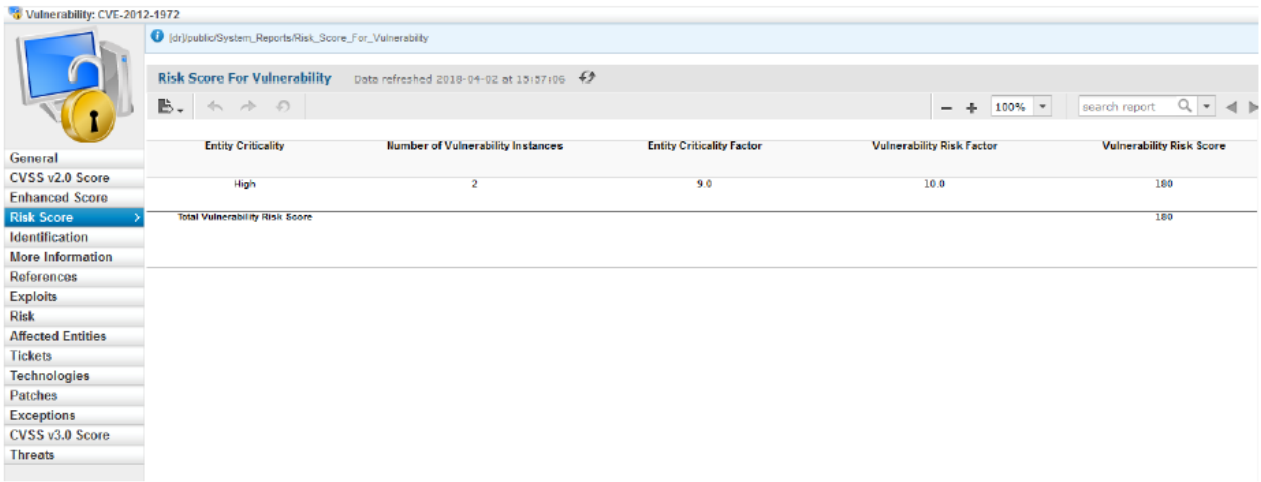
The Vulnerability Risk Score appears in the following locations within the RiskVision user interface:

- The following vulnerability grids have a new risk score column: Vulnerabilities from Scanners or Users, Scanner & Inferred Vulnerabilities, All Vulnerabilities, Recent Vulnerabilities, and Recent Vulnerabilities of Interest.

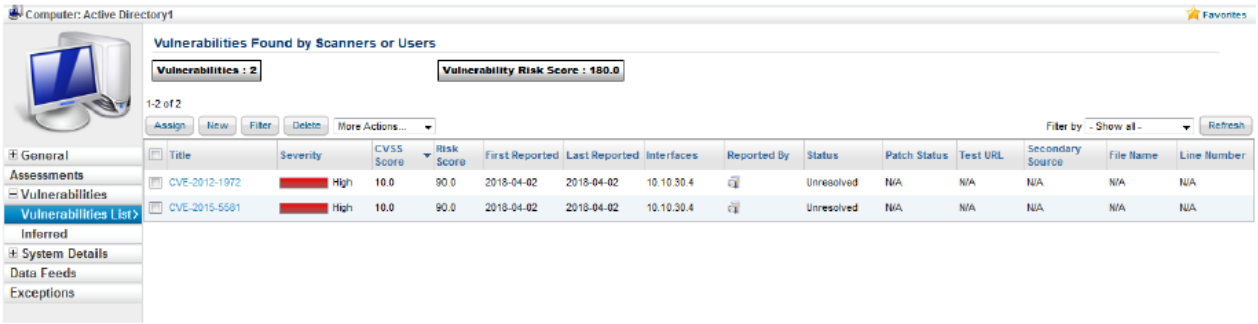


- The vulnerability definition and vulnerability instance user interfaces have two new tabs: Enhanced Score and Risk Score. The Enhanced Score tab shows the components of the Enhanced Risk Score as well as the overall Enhanced Score. The Risk Score tab shows the components of the Entity Criticality Factor, Vulnerability Risk Factor, and Vulnerability Risk Score. For the vulnerability definition, these tabs show the totals across all instances of the vulnerabilities, while the instance only shows the scores for that instance.





- The Vulnerabilities List tab that appears in certain types of entities, such as computers and applications, has a new Risk Score column. Additionally, it shows an aggregate vulnerability Risk Score for the entity at the top of the tab, above the grid.



Null Values

When a variable that's used for the vulnerability risk score calculation is not present, this results in a null value, which will nullify the result of the vulnerability risk score equation. The only exception to this is when a vulnerability does not have any mapped exploits, in which case the Exploit Factor of the Enhanced Score is given a value of .25.

Null values are displayed in the **Enhanced Score** and **Risk Score** tabs as “N/A.”

Configuring the Vulnerability Risk Score Calculations

Please refer to the Administrative Guide for the instructions regarding configuring vulnerability risk score calculations.