FAQs for CVSS v2 Customers

Question	Answer
When will Veracode deprecate CVSS v2?	Veracode will be moving customers from version 2 of the Common Vulnerability Scoring System (CVSS) to version 3 in batches. Your Customer Success Manager (CSM) will provide an exact date. The last batch will be in December 2023. The official end of life (EOL) date is April 1st, 2024.
Can I switch to CVSS v3 now?	Yes. Please email support@veracode.com and ask that the CVSSv3 feature be activated for your account.
How long has the CVSS v3 feature switch been available?	The CVSS v3 feature switch has been available since Oct 2019.
Why is Veracode deprecating CVSS v2?	There are several reasons: 1) CVSS v2 is 16 years old, 2) CVSS v3 is 8 years old, 3) NVD retired v2 in July 2022, 4) customer demand for v2 support has dropped, 5) supporting one version will pave a faster road to unifying the SCA agent and SCA upload scanners, and 6) NVD expects to begin introducing components of CVSS v4 in 2023.
Will this change impact SCA Upload or SCA Agent or both?	Initially, when Veracode activates the CVSS v3 feature switch, it will only impact SCA Upload scans. We encourage customers who use SCA Agent scans, however, to update their agent rules to use CVSS v3 severities because as Veracode works to merge the two scanning technologies, support for CVSS v2 will eventually cease on the SCA Agent side as well.
Is there a report that I can run to understand the impact of this change on my SCA results?	Yes. Your CSM can share a report with you. We are working on adding it to Analytics so that all customers can self-serve and run it without involving their CSM.
What severities are displayed by default?	By default, Veracode takes the CVSS v2 score (number) and converts it to a severity rating (text), based on what range the score falls into. The default range, which can be found here in the help center, is proprietary to Veracode and was established before version 3 of CVSS was released.

<table>
<tr><th>Question</th><th>Answer</th></tr>
<tr><td>How can I tell whether I am using CVSS v2?</td><td>If your SCA Upload scan results display a severity of "High" for CVE-2016-1000027, CVE-2022-22965, CVE-2022-1471, or CVE-2019-16942, then your account is configured to use CVSS v2. If they show a severity of "Very High," then you are using CVSS v3. Alternatively, you can email support@veracode.com and ask whether CVSSv3 is ON or OFF for your account.</td></tr>
<tr><td>CVSS v2 normally has only 3 levels of severities, but I see more, am I using CVSS v3?</td><td>Not necessarily. The Veracode platform currently uses a proprietary method to convert the underlying score for a CVE into a severity, such as Very High, High, Medium, Low, or Informational. As shown in the table below, there is some similarity between Veracode's proprietary ranges and the CVSS v3 ranges used by the NVD, which are published here, so the impact of migrating from v2 to v3 should be lower than it would be otherwise.
<table>
<tr><th>Severity</th><th>Veracode-proprietary ranges for CVSS v2</th><th>Standard NVD ranges for CVSS v3</th></tr>
<tr><td>Very High</td><td>8.1-10.0</td><td>9.0-10.0</td></tr>
<tr><td>High</td><td>6.1-8.0</td><td>7.0-8.9</td></tr>
<tr><td>Medium</td><td>4.1-6.0</td><td>4.0-6.9</td></tr>
<tr><td>Low</td><td>2.1-4.0</td><td>0.1-3.9</td></tr>
<tr><td>Very Low</td><td>0.1-2.0</td><td>n/a</td></tr>
<tr><td>Informational</td><td>0.0-0.0</td><td>0.0-0.0</td></tr>
</table></td></tr>
<tr><td>Will my results change immediately?</td><td>The severities for each SCA finding will change immediately after Veracode Support activates CVSS v3 for your account, but the pass/fail status of an application will not change until Veracode runs a policy re-evaluation job. Policy re-evaluations for customers making feature switch changes are scheduled for 8 PM Eastern US time and utilize the latest policy scan for each app to perform the re-evaluation.</td></tr>
<tr><td>Will the pass/fail shield change?</td><td>The shield next to each finding will change immediately, but the shield next to the app will not change until Veracode runs a policy re-evaluation job. Policy re-evaluations are scheduled for 8 PM Eastern US time and utilize the latest policy scan for each app to perform the re-evaluation.</td></tr>
</table>

Question	Answer
What if we use a custom policy that evaluates vulnerability score instead of severity?	Veracode Policies are version-agnostic, so the evaluation of your results will not change. But since the underlying score of each CVE will change, you can expect some changes in pass/fail status.
What happens when NVD publishes a v3 score but not a v2 score?	When the NIST does not publish a v2 score, Veracode's research team will calculate it using NVD's CVSS v2 Calculator before adding the CVE to our vulnerability database. In the end, all vulnerabilities in Veracode's database have both a v2 score and a v3 score. (These scores are numbers between 0 and 10.)
Does the CVSSv3 switch impact agent scans?	No. None of the feature switches in the platform impact agent scans; they only impact upload scans. Customers who want their agent scans to use CVSS v3 for scoring must update their workspace rules. Since setting up new rules for every workspace can be time-consuming, Veracode recommends using org-level rules to force all workspaces to use v3 scoring.
Does Veracode use version 3.0 or 3.1?	Veracode uses version 3.1, but users will not notice the difference because 1) Veracode only uses the base score and 2) there really is no difference between a v3.0 base score and a v3.1 base score.
Will grace periods be extended after switching from CVSS v2 to v3?	No. Grace periods are based on the first found date, which is not impacted by changing the score. Using grace periods, however, is an excellent strategy for navigating the transition from v2 to v3. Specifically, since users may see a sudden increase in High or Very High Severity vulnerabilities after switching from v2 to v3, Veracode recommends temporarily increasing grace periods to give developers more time to address the sudden influx of issues.
When will Veracode support CVSS v4?	CVSS v4 is not expected to be officially published until September 2023, so Veracode is not likely to add support for v4 until 2024 at the earliest. For more details, see https://www.first.org/cvss/v4-0.