Transition from OVAL to VEX Files for Red Hat Security Data

Summary

As part of our ongoing commitment to provide precise and up-to-date vulnerability data, Prisma Cloud is transitioning from the OVAL format to the VEX format for assessing vulnerabilities in Red Hat artifacts. This change affects how vulnerabilities in Red Hat products and artifacts are reported in Prisma Cloud environments.

Until you upgrade to a 33.xx release, Prisma Cloud will continue to use the OVAL format for vulnerability scanning, with no expected impact. After upgrading your Console and Defenders to version 33.00 (or later), Prisma Cloud will start using the enhanced and detailed reporting capabilities of the new VEX format.

Prisma Cloud will also support OVAL files for another two major versions— v33.xx and v34.xx—to maintain compatibility with Defenders in the pre-33.xx releases, as long as Red Hat continues to support and produce them.

This document explains the changes for customers upgrading their Console and Defenders to 33.00 and later releases. For customers who do not upgrade their Defenders and Console, no changes in behavior and reporting are expected.

If you have any concerns or need more information about this transition, please contact: support@paloaltonetworks.com.

Background and Motivation

- Red Hat security data is the primary source for known and published vulnerabilities in Red Hat products.
- Red Hat was previously using the OVAL and CVRF data formats to provide security information about Red Hat products.
- Prisma Cloud consumed Red Hat OVAL v2 files to enrich the Intelligence Stream feed and provide accurate reporting on vulnerabilities in Red Hat products.
- The security data landscape is constantly changing, necessitating improvements to meet new industry standards and customer requirements. Red Hat announced that the official Red Hat vulnerability data will be available in a new format called the Vulnerability Exploitability eXchange (VEX).

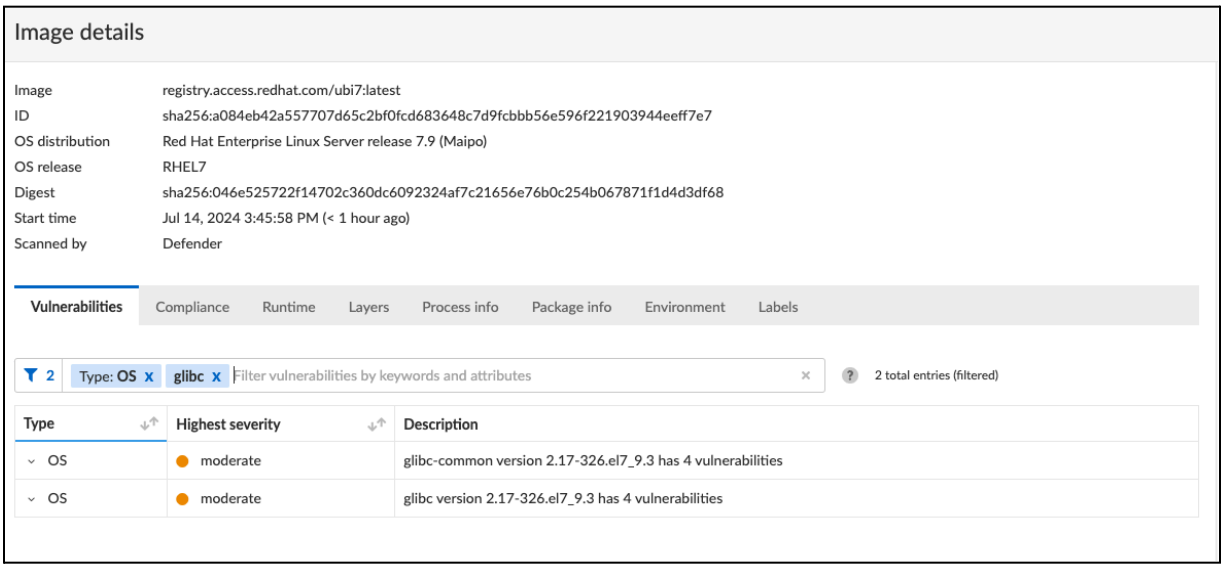
- On July 10, 2024, Red Hat announced general availability of VEX files for CVEs and moved the support for OVAL v2 to maintenance mode. The OVAL format will not receive any new features and updates will be limited to critical bug fixes only.
- To consume the latest updates on Red Hat vulnerabilities in the long term, Prisma Cloud needs to use the new VEX format.

Changes in the VEX Format

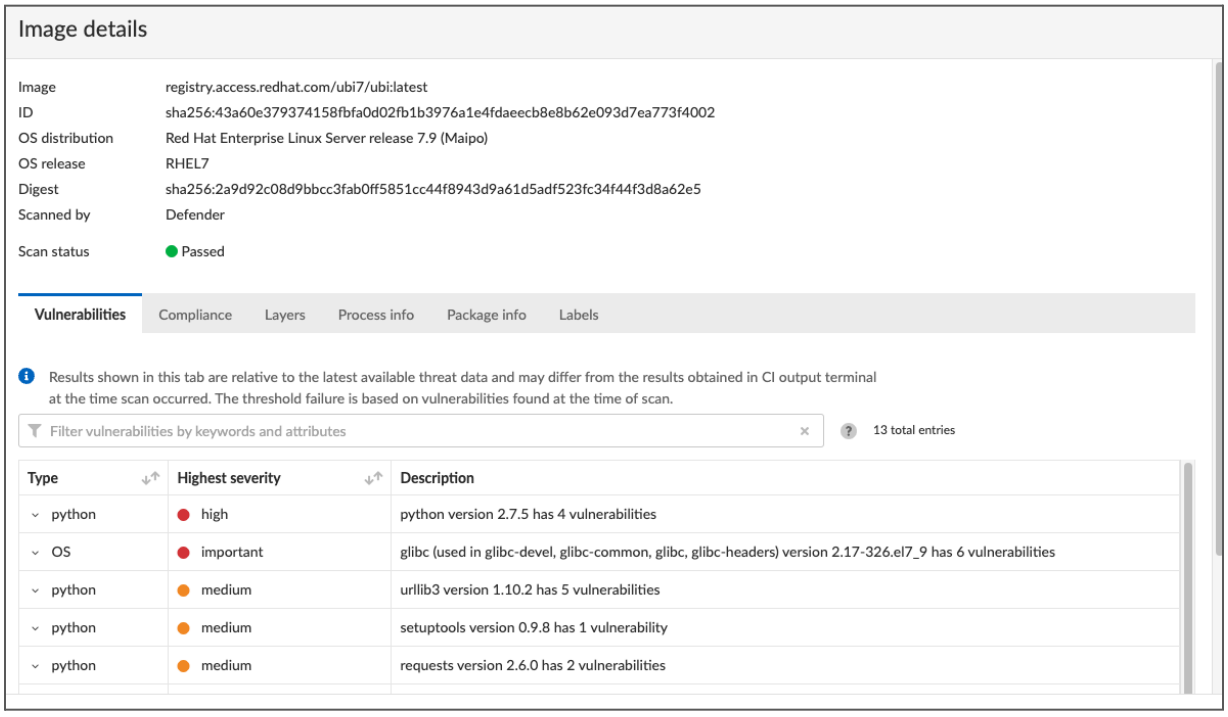
- With OVAL files, Red Hat provided information on vulnerable RPM packages and all associated binaries built from those packages, irrespective of their vulnerability status ("Fixed," "Known Affected," "Known Not Affected," and "Under Investigation").
  For example, if a vulnerability was found on a package with the CVE status “Under Investigation”, Red Hat would publish the vulnerability information for affected binaries as well.
- With the VEX files, Red Hat provides vulnerability information for the vulnerable RPM packages for all the vulnerability statuses, but only publishes vulnerability information for the affected binaries only when a fix is available.
- With the OVAL files, Prisma Cloud reports a CVE for each affected binary and RPM package found during the scan. For example, if a source package with a vulnerability was included in two binaries, Prisma Cloud would report two CVEs—one for each binary.
- Prisma Cloud now adopts a new reporting mechanism aligned with the VEX format. It will report one record for the RPM package as vulnerable, and provide information on all the detected binaries built with it.

Comparison (Example)

With the OVAL format, Prisma Cloud reported a vulnerability for each binary found during the scan. For example, the **glibc-common** and **glibc** binaries as shown in the following screenshot.



With the new VEX format, Prisma Cloud reports one vulnerability only for the source package, and provides information on the related binaries. For example, the **glibc** package (used in binaries: **glibc-devel**, **glibc-common**, **glibc**, **glibc-headers**) as shown in the following screenshot.



With VEX logic, the number of vulnerabilities with the same CVE-ID will be reduced, as Prisma Cloud will report a single vulnerability for the RPM package instead of multiple reports for each binary.

Comparative Metrics for OVAL and VEX Formats

For details on how CVEs are reported in the new VEX format as compared to the OVAL format, see CVEs Comparison between Oval and VEX.

FAQs

1. Will I see more vulnerabilities?

   In general you should see a reduction in the number of vulnerabilities, as Prisma Cloud's new reporting mechanism for Red Hat vulnerabilities is based on the RPM package and will report only one vulnerability per package instead of several vulnerabilities for each binary. However, VEX CVE files report more vulnerabilities and provide more detailed information for each vulnerability. So the total number of vulnerabilities might increase, but are expected to be in the same range as earlier overall. The increase is mainly observed for CVEs with 'Medium' and 'Low' severities.

2. If I don't upgrade my console, could I miss out on addressing new or existing vulnerabilities?

   No. For customers who do not upgrade their Console and Defenders, Prisma Cloud will continue to use OVAL information for vulnerabilities and the report will be exactly the same.
   However, OVAL files have been moved to maintenance mode. According to Red Hat blog: "Red Hat will continue to produce OVAL v2 content for core products such as Red Hat Enterprise Linux (RHEL) 8 and 9, but OVAL data won't receive new features and will be limited to critical bug fixes only. OVAL content will not be published for future major RHEL releases (10 and onward) as well as any new products".
   This might result in a gap between the OVAL and the VEX security content. Customers who upgrade their Console and Defenders to v33.xx will not experience this gap, as Prisma Cloud will use the VEX security information to report Red Hat vulnerabilities.

3. What will be the impact on the number of vulnerabilities I have?

   When using the new Console and Defender version, the total number of vulnerabilities might increase as "new" vulnerabilities might be reported by Red Hat on the VEX files that were not included on the OVAL files.. The number of records of the same CVE-ID will reduce as Prisma Cloud will report only one vulnerability for the RPM package instead of several recordings for each binary that is sourced from the RPM package. When using old Defenders, you will not see any impact.

4. What will be the impact if I don't upgrade my Defenders to version 33.xx?

   There will be no change in behavior and no impact is expected. For old Defenders, Prisma Cloud will continue to use the OVAL format to report vulnerabilities. Prisma Cloud will continue to consume the OVAL files for another two major versions— v33.xx and v34.xx—to maintain compatibility with Defenders in the pre-33.xx releases, as long as Red Hat continues to produce OVAL files. When version 32.xx reaches end of support, Prisma Cloud will stop using OVAL files.

References

For additional details on VEX files from Red Hat, see the following Red Hat blogs:

- Red Hat announcement on the general availability of VEX files: https://www.redhat.com/en/blog/red-hat-vex-files-cves-are-now-generally-available
- Red Hat VEX structure and motivation: https://www.redhat.com/en/blog/vulnerability-exploitability-exchange-vex-beta-files-now-available