



CodeSentry Release Notes

Current Version

CodeSentry 7.1 Release Notes

What's new in CodeSentry 7.1?

Watch the CodeSentry 7.1 new feature introduction video here! [CodeSentry 7.1 New Feature Walkthrough](#)

- **Instance-Wide SBOM Policy**
 - CodeSentry now features an instance-wide SBOM Policy setting. The policy can be set to automatically exclude discovered components based on match confidence.
- **VEX Export**
 - Corrected an error with VEX annotations.
- **User Interface Changes**
 - Page name changes
 - Vulnerability Filter (previously "EPSS/KEV Filter")
 - License Policy (previously "License Policies")
 - New Scan dialog modified.
 - New **SBOM Policy** toggle.
 - Vulnerability toolbar modified. (available in Summary: Vulnerabilities tab and Scan Results: N-Day Findings tab).
 - The vulnerability filter toggle is now labeled **Vulnerability Filter** (previously "Instance Wide Vulnerability Filter").
 - CodeSentry Settings menu modified.
 - Two items have been renamed in line with the renamed pages they link to: License Policy (previously "License Policies") and Vulnerability Filter (previously EPSS/KEV Filters)
 - One new item: SBOM Policy
- **Updates to Vulnerability Information**
 - CodeSentry 7.1 includes over 6,000 new vulnerabilities and 2,600 new products.

Previous Versions

CodeSentry 7.0 Release Notes

What's new in CodeSentry 7.0?

Watch the CodeSentry 7.0 new feature introduction video here! [CodeSentry 7.0 New Feature Walkthrough](#)

- **Access Control: RBAC and GBAC**

- There are now three basic user types: Admin User (administrative privileges), Manager User (extended privileges) and Standard User (basic privileges). Special groups `codesentry_manager` and `codesentry_sysadmin` confer Manager User and Admin User status, respectively. You can change membership for these groups, but do not rename or delete them.
- Application visibility depends on user status.
 - Admin Users and Manager Users have full access to all applications.
 - For Standard Users, access to applications is managed with *Group-Based Access Control (GBAC)*.
- A new Manage Applications page manages application visibility for Standard Users. Assign a group to an application to specify that Standard Users can only access the application if they are in that group; set the application to have no assigned group to specify that no Standard Users can access the application.
- The user management tools now include functionality for assigning users to groups and for creating new groups.
- A new `Default Group` group is provided. This group is entirely under your control: you can change its membership, rename it, or even delete it entirely.
- This manual has been updated to note the user status required to access CodeSentry UI pages and functionality.
- If you are upgrading:
 - All existing Admin Users remain Admin Users, and are members of the `codesentry_sysadmin` group.
 - All other existing users become Manager Users, and are members of the `codesentry_manager` and `Default Group` groups.
 - All existing applications are assigned the `Default Group` group.
- Newly registered users are created as Manager Users, and are members of the `codesentry_manager` and `Default Group` groups. Admin Users can change this behavior through the Realm settings: see Specify Default Groups for New Users.
- The New Scan dialog now contains a Group Assignment field.
 - When you add a new scan to an existing application, this field displays the application's assigned group.
 - When you create a new application for a new scan, this field allows you to specify the application's assigned group.

For more information, see Access Control: RBAC and GBAC.

- **Instance-Wide Vulnerability Filtering**

- Each CodeSentry instance now has an instance-wide EPSS/KEV filter setting.
- With factory settings, there are no filter conditions: all vulnerabilities pass the filter.
- The current setting can be viewed (all users) and modified (Admin Users only) from the new EPSS/KEV Filters page.
- The filter is *always* applied to the Dashboard. This affects the contents of the Organization Security Rating, N-Day Findings, and N-Day Findings Heat Map widgets.
- The Summary: Vulnerabilities tab and Scan Results: N-Day Findings tab both provide an **Instance-Wide Vulnerability Filter** toggle so that their respective tables of vulnerabilities can be viewed both with and without filtering.

- **GUI**

- There is a new CodeSentry Settings menu in the main toolbar.
 - Manage Users is now in this menu, when available. (Previously it was in the User Settings menu.)
 - The CodeSentry Settings menu also provides links to the new **EPSS/KEV Filters**, **License Policies**, and **Manage Applications** pages.
 - The New Scan dialog now contains a Group Assignment field.
 - There are several new pages.
 - Manage Applications
 - License Policies
 - EPSS/KEV Filters
 - The Scan Results and Summary pages now contain an **Instance-Wide Vulnerability Filter** toggle, controlling whether or not the instance-wide EPSS/KEV filter is applied.
 - The Dashboard now always has the instance-wide EPSS/KEV filter applied.
- **License Policies**
 - Each license type now has an instance-wide *license policy* specifying the default state (*Not Approved*, *In Review*, or *Approved*) of that license in each associated component instance.
 - You can view and modify license policies on the new License Policies page. All users can view license policies on this page; only Admin Users modify policies.

- **Compact N-Day Findings**

Reported N-Day findings are now grouped by Vulnerability ID, Component Name, and Component Version.

- GUI: Scan Results: N-Day Findings
 - The main table in each of these tabs now contains one row for each (vulnerability, component name, component version) triple.
 - When a row in the main table is expanded, the expanded entry contains summary information about the vulnerability and a vulnerability-target table with one row for each occurrence of the vulnerability in a scanned target. This table includes some columns that were previously in the main table: **Match**, **Status**, and **Annotate**.
 - When a row in the vulnerability-target table is expanded, the expanded entry contains the MD5, SHA-1, and SHA-256 hashes of the target along with vulnerability occurrence details.
 - GUI: Summary: Vulnerabilities The same structural changes as described above for Scan Results: N-Day Findings. The new vulnerability-target table includes a link to the corresponding Scan Results.
 - GUI: Dashboard
 - N-Day Findings and N-Day Findings Heatmap reflect per-component max severity and max match level
 - The Organization Security Rating calculation has now been updated to reflect the max CVSS scores of unique Components by Name and Version.
- **Updates to Vulnerability Information**
 - CodeSentry 7.0 includes over 8,300 new vulnerabilities and 5,000 new products.

- **Vulnerability Annotation**

It is no longer possible to annotate multiple different vulnerabilities in a single operation. You can still annotate multiple occurrences of the same vulnerability in a single operation.

- **N-Day Findings Justification**

- A CycloneDX **Justification** may now be set for N-Day Findings which are annotated as **Not Affected**. This justification will be included in CycloneDX VEX exports and Scan reports.

- EPSS and KEV List
 - EPSS score and CISA KEV list inclusion values are now displayed and filterable on the N-Day Findings tab, and included in the **N-Day Findings Details** section for the Scan report.
- Deep Zero-Day Analyzer Removed
 - Following the deprecation in CodeSentry 6.1, the Deep Zero-Day analyzer has been removed, and deep Zero-Day scans can no longer be performed.
 - Performing new **shallow** Zero-Day scans will continue to be supported, using the UI or API.
 - Results for existing deep Zero-Day scans will continue to be available, both in the UI and API.
 - Documentation for deep Zero-Day scans has been removed (other than release notes), and documentation references to "shallow" Zero-Day scans have been changed to simply refer to Zero-Day scans.

CodeSentry 6.2 Release Notes

What's new in CodeSentry 6.2?

Watch the 6.2 new feature video here! [CodeSentry 6.2 SaaS New Feature Walkthrough](#)

- When exporting CycloneDX without files, duplicate components are consolidated. If a CycloneDX 1.5 export is requested, target file occurrences will be emitted in the component **occurrences metadata**.
- When an installed package detected by Operating System Analysis contains additional text in the component name such as padding spaces or its version string, this is removed before reporting the components.
- Bug Fixes
 - A bug has been fixed in the CycloneDX export when directly adding the same component multiple times: identical entries will be consolidated, and distinct entries will be distinguished by unique **bom-ref**s.
 - A bug has been fixed where component CPEs in exports contained an **a** in the "part" field for all components, rather than a more suitable value. The "part" field can now be any of the following three values:
 - **a** when the component is an application
 - **o** when the component is an operating system
 - **h** when the component is a hardware device

CodeSentry 6.1 Release Notes

What's new in CodeSentry 6.1?

Watch the 6.1 new feature video here! <https://youtu.be/jZrdbwkwG8Q>

- User Interface Changes
 - The Bill of Materials tab now groups components with identical name, version, and vendor values to reduce the number of rows that differ only by file path.

- The Bill of Materials tab Annotate functionality can now be used to modify the state (**Included** or **Excluded**) and add a comment for multiple components at a time.
- The Scan Report now includes an N-Day Finding Annotations section.
- When a user performs any of the following actions, their email is logged with other information about the action.
 - Start a new scan.
 - Directly add a component.
 - Add or modify a vulnerability annotation (only the user responsible for the most recent change is saved).
 - Add or modify a component annotation (only the user responsible for the most recent change is saved).

For any of these actions taken prior to CodeSentry 6.1, the user responsible for the action will display as "CodeSentry User".

- Logged email addresses are displayed in the Scan Report and User Interface to identify the users who performed various actions. The following User Interface pages have been extended to support this purpose: the email of the user who created the scan is displayed on the Scan Status Tab and on the Scans Tab, the email of the user who last annotated a component or directly added a component is displayed on the expanded row of the component on the Bill of Materials Tab, and the email of the user who last annotated a vulnerability is displayed in the **Vulnerability Details** section of an expanded row on the N-Day Findings Tab.

- **Operating System Analysis**

- The new **operating system analysis** detects the operating system (OS) version and software packages installed within a Windows disk image.
- See Understanding the Operating System Analysis for detailed information on the supported file types and the form of the results.

- **N-Day Analysis (and SBOM Edition)**

- When license names contain quotation marks, CodeSentry now uses single quotes consistently. (Previously, double quotes were sometimes used.)

- **WIM/SWM Archive Support**

- Single and multi-volume WIM (Windows Imaging Format) archives (**.wim** , **.swm**) are now supported. See note for details.

- **Exports**

- The Bill of Materials CSV export now includes a Match Confidence column.

- **Documentation Change**

- The manual now includes instructions for upgrading an on-premise airgap installation via the user interface.

- **Updates to Vulnerability Information**

- CodeSentry 6.1 includes over 8,500 new vulnerabilities and 6,300 new products.

- **API Additions**

- Vulnerability EPSS scores are now available in the **vulnerability_found_search** and **vulnerability_headers** queries.
- The API now provides access to KEV catalog information for detected vulnerabilities. See this link for more details.
- The **metrics** API **scan.status** field, and the **scan_status** API **abridged_scan_state** field will now return **"Analyses Completed"** when in the state previously referred to as **"Collating"**

- **Updated Kubernetes**
 - SaaS Kubernetes Cluster upgraded to version 1.29.5.
- **Zero-Day Deep Scan Deprecation**
 - Deep Zero-Day scans are now deprecated, and may be removed from the product in the future. CodeSecure does not recommend that users continue to perform Deep Zero-Day scans.
 - Zero Day shallow scans will continue to be supported, using the UI or API.
 - Results for existing zero-day scans will continue to be available in the UI.
- **Bug Fixes**
 - An issue, where an error appears when opening the vulnerability annotation dialog for a vulnerability without a vulnerability description, has been fixed.
 - Scan Status job counts now consistently reflect analysis job counts without including vulnerability database update job counts.
 - The instance dashboard is now responsive to browser widths.
 - Very large archives are now unpacked more reliably.

CodeSentry 6.0.1 Release Notes

- **Large Scan Load Performance Improvement**
 - The load time of large scans has been improved

CodeSentry 6.0 Release Notes

- **User Interface Changes**
 - The N-Day Findings tab now includes an **Annotate** option which provides functionality for changing vulnerability **Status** and modifying **CVSS Score** values. See Edit or Modify a Bill of Materials for examples of this new functionality. Note that this functionality is also available on the Vulnerabilities tab.
 - If you apply vulnerability annotations, the Bill of Materials tab expanded details view now organizes vulnerabilities by **Status**.
 - Search filters applied on the Summary page are now applied to the URL, making URLs with specific search results easy to share.
 - The N-Day Findings tab now includes a **Match Level** filter.
 - The Components tab now includes **Pass/Fail** status and **License Risk** filters.
 - The **Dashboard** and **Summary** links in the Menu panel are now fixed in place to improve ease of navigation.
 - Widgets on the Dashboard have been updated to be more interactive. Clicking certain elements on the dashboard now open the appropriate view on the Components tab and Vulnerabilities tab.
 - The user interface now displays file size in base-2 format.
 - Several error messages have been made more informative.
 - To improve security:

- User messaging related to an incorrect username or password no longer specifies which value is incorrect, and has been changed to say that one of the values is incorrect.
 - Idle and max session lifetimes have been reduced to conform to security best practices.
 - The scan status *Analyses Completed, Results Not Collated* has been replaced by status *Scan Done* in the user interface. Note that the API still displays a status of *Collating*.
- **Note on License Expiry**
 - Licenses expire at 11:59:59 EST on the expiration date.
- **Adjustment of Remaining Licensed Scan Count**
 - Under some common failure scenarios, consumed licensed scans will be credited back to the remaining licensed scans.
- **File Size Limits**
 - This release introduces changes to maximum file size and archive expansion limits.
 - ISO files containing uncompressed data up to 40GB.
 - Archive file types with compressed data (whether uploaded directly or extracted from an archive): up to 7GB.
- **Documentation Change**
 - There is a new page called Video Archive that includes links to New Feature videos and Tutorials from past CodeSentry releases.
 - The manual now includes a **Back to Top** button that automatically scrolls large pages to the top.
 - Accessing the manual now requires authentication.
 - The CodeSentry login screen now includes **Forgot password?** help text.
- **Bug Fixes**
 - This release includes several bug fixes, including:
 - An issue on the New Scan dialog in which application names were not appearing in the autocomplete suggestion list if an application had more than 50 scans, has been fixed.
 - An issue where CVEs could potentially be disassociated from a vulnerability has been fixed.
 - Fixed an issue on the N-Day Findings tab to ensure that when users change the table filter and the number of rows is reduced, the pagination adjusts to reflect the actual number of pages available.
 - Minor issues with the Add Component feature have been fixed to improve usability.
 - An issue where the Scan Quality score displayed in the user interface sometimes did not match the value displayed in the Scan Report, has been fixed.
 - An issue where the **Solution** displayed on the N-Day Findings tab and related dashboard widget displayed **Null**, has been fixed.
 - The Scan Report tab could be slow to respond for large scans. It now displays a loading icon in these scenarios.
 - An issue where the Overall Security score did not immediately update when navigating between scans in the user interface, has been fixed.

- Made the system more robust in the case of error conditions, by removing a case where analysis jobs could be lost, preventing a scan from completing.
 - A bug, where a product could sometimes not be added via product lookup if an application has more than 100 scans, has been fixed.
 - A bug, where certain products could not be added via product lookup, has been fixed.
- **Analysis Engine Updates**
 - Ongoing improvements and refinements to the CodeSentry analysis engine will result in changes to reported components and vulnerabilities compared to previous versions of CodeSentry.
 - **Updates to Internal Components**
 - Certain internal packages, including Angular and Moment.js, have been upgraded.
 - **Updates to Vulnerability Information**
 - CodeSentry 6.0 includes over 18,800 new vulnerabilities and 7,800 new products.
 - **Updated Kubernetes**
 - SaaS Kubernetes Cluster upgraded to version 1.27.
 - **Deep Zero-day Analysis Change**
 - Zero-day deep analysis no longer supports PowerPC. Support remains for x86, x64, ARM64, and ARM/Thumb binaries.
 - **Security Attributes Analysis Changes**
 - The Security Attributes analysis now reports a RELRO score of **N/A** for ELF shared libraries. This attribute is not applicable to libraries.
 - **Added Support**
 - The following Linux distributions/versions are now supported for CodeSentry installation as of this release.
 - Ubuntu 22.04.
 - Red Hat Enterprise Linux Server v8.7-9.3.
 - CentOS 8 Stream.
 - **Deprecation Notices**
 - The following Linux distributions/versions are no longer supported for CodeSentry installation as of this release.
 - RedHat Enterprise Linux Server v7.4.
 - CentOS v7.9.

CodeSentry 5.2 Release Notes

- **CodeSentry Rebranding**
 - CodeSentry is now a product of [CodeSecure, Inc.](#)
- **Notes on Upgrading**

- Upon upgrade, system performance may initially be reduced while existing scans are updated; the duration of this initial update will depend on the size and age of the CodeSentry instance.
- **User Interface Changes**
 - There is a new License Findings tab in the user interface. Use this tab to review and approve licenses that govern the usage of discovered components.
 - The *Component Annotation* feature has expanded to include license findings. You can annotate licenses as **Approved**, **Not Approved**, or **In Review** (note that **In Review** is the default state) and bulk annotate multiple licenses at once.
- **Component Match Details**
 - The Component Match Details dialog has been improved to display additional match detail information. You may now also download a JSON file with all match details for a given component.
- **CWE Top 25 Update**
 - Zero-Day finding scoring has been updated to reflect the [2023 CWE Top 25](#) list.
- **Archive Types**
 - CodeSentry can now handle additional SquashFS file types: `.squashfs` , `.sfs` , `.sqf` , `.sqfs` , `.sqs` , `.squ` .
 - Improved support for POSIX `.tar` files.
- **Bug Fixes**
 - This release includes several bug fixes, including:
 - An issue where HTML reports were not being returned for large reports in sites without the Vulnerability Database Update service has been fixed.
 - An issue where some dialog text was difficult to see in dark mode has been fixed.
 - An issue where a user could see the error `Cannot read properties of undefined (reading 'forEach')` upon selecting the **HTML as ZIP** option on the Scan Report tab has been resolved.
- **CycloneDX Export Change**
 - The CycloneDX export has been changed to include a license `id` field instead of a license `name` field.
- **Analysis Engine Updates**
 - Ongoing improvements and refinements to the CodeSentry analysis engine will result in changes to reported components and vulnerabilities compared to previous versions of CodeSentry.
 - Improvements in resource allocation have reduced the instances of failed analyses of target files near the upper limit of 200MB.
- **CVE ID Association Improvements**
 - All available CVE IDs associated with a detected vulnerability are now displayed. Formerly, CVE IDs were only displayed if the CVE had received a CVSS score from the NVD.
- **Documentation Change**
 - There is a new overview page called `How Do I...?` that lists common CodeSentry activities and links to the appropriate reference material in the manual.

- **Updates to Vulnerability Information**

- CodeSentry 5.2 includes over 3,500 new vulnerabilities and 1,600 new products.

- **Deprecation Notices**

- The following Linux distributions/versions are no longer supported for CodeSentry installation as of this release.
 - CentOS v7.2.
 - Debian - all versions.
 - openSuse - all versions.
 - Suse Linux Enterprise - all versions.
- RedHat Enterprise Linux Server v7.4-7.8 will no longer be supported in CodeSentry 6.0.
- See the current list of officially supported Linux distributions [here](#).

CodeSentry 5.1.1 Release Notes

- **Changes to Exports**

- CycloneDX
 - A bug in CycloneDX generation was fixed.

CodeSentry 5.1 Release Notes

- **Notes on Upgrading**

- If Deep N-Day scans are in progress, please wait until these scans complete before initiating the upgrade. If you upgrade while Deep N-Day scans are in progress, the in-progress scans will be permanently in the **Queued** state and appear to be indefinitely stuck on the **Scanning** state, unable to complete.
- Upon upgrade, system performance may initially be reduced while existing scans are updated; the duration of this initial update will depend on the size and age of the CodeSentry instance.

- **Introducing Vulnerability Updates**

- CodeSentry 5.1 introduces vulnerability updates for connected instances (SaaS and On-Premise with internet access). New and updated vulnerabilities will be synchronized to your instance on an ongoing basis.

- **Component Reporting Improvements**

- This release of CodeSentry improves the handling of some additional archive formats (self-extracting executables, for example) such that discovered components can be associated with the actual target file inside the artifact. For these formats, **Security Attributes** and **Zero-Day** results will be run only on the archive itself. A future CodeSentry version will fully handle these archive types.

- **Updates to Vulnerability Information**

- CodeSentry 5.1 includes over 8,400 new vulnerabilities and 3,900 new products.

- **FIPS Compatibility**

- Certain internal packages, including Keycloak, have been upgraded to be compatible with FIPS environments.

- **Dependency Analysis**
 - When performing an analysis, CodeSentry determines the immediate shared library dependencies of Windows and Linux. Results are available on the newly added External Dependencies tab of the user interface and in the **External Dependencies** section of the Scan Report. Windows and Linux are currently supported. Other platforms may be supported in a future version.
- **User Interface Changes**
 - The **Add Product** feature is now named **Add Component**.
 - The user interface lists vulnerability update timestamps on the Vulnerabilities tab and the About CodeSentry page.
 - The New Scan dialog has been updated.
 - You may now select an **Artifact Type** and specify an **Artifact Version**.
 - These new fields are reflected in the Bill of Materials and related exports.
- **HTML Scan Reports**
 - If you require a Scan Report for a very large scan that exceeds PDF generation limits, you may now download the Scan Report in HTML format. Use the **HTML as ZIP** option on the Scan Report tab. Some scans may be too large to export as HTML via the user interface. In these cases, use the API to retrieve scan data.
- **Changes to Exports**
 - **SPDX**
 - There is now an option to download the SPDX bill of materials in JSON format. This can be done via the API and the user interface.
 - The SPDX Tag format has been updated to SPDX version 2.3.
 - **CycloneDX**
 - There are new options allowing users to include or exclude the list of scanned files in the CycloneDX export. This can be done via the API and the user interface.
 - Directories and folders are no longer listed as files in CycloneDX exports.
 - This version of CodeSentry supports CycloneDX v1.5. The default value for exports via the user interface and API remains v1.4. You can retrieve a v1.5 CycloneDX bill of materials via the API.
 - **CSV**
 - There are additional CSV endpoints for retrieving additional result entities. You may now Get the Scan's N-Day Vulnerability Listing, Get the Scan's External Dependency Listing, Get the Scan's Security Attribute Listing, and Get the Scan's Zero-Day Warning Listing.
- **Update to Analysis Types**
 - Deep zero-day jobs are now created through the new **zero-day-deep** analysis type, which should not be combined with **zero-day** type jobs.
 - The analysis type **thoroughness** has been removed from the API.
- **New Match Score Algorithm**

- This release of CodeSentry introduces an improved match level algorithm. As a result, new scans performed with v5.1 may return different match levels for the same components discovered with older CodeSentry versions.

- **Analysis Engine Updates**

- Ongoing improvements and refinements to the CodeSentry analysis will result in changes to reported components and vulnerabilities compared to previous versions of CodeSentry.

CodeSentry 5.0 Release Notes

- **Dependency Analysis**

- When performing a Security Attributes analysis, Linux shared libraries now have their **SONAME** field reported to CodeSentry, if present. This value is available via the API. This information will be available via the user interface in a future version.
- When performing an analysis, CodeSentry determines the immediate shared library dependencies of Windows (**PE**) and Linux (**ELF**). The results are available via the API. This information will be available via the user interface in a future version.

- **User Interface Changes**

- There is a new Vulnerabilities tab on the Summary page. This page lists the complete set of vulnerabilities discovered by all scans performed on your instance, and provides various search options for finding scans which include specific vulnerabilities.
- The Bill of Materials tab now includes an **Annotate** option which provides functionality for excluding components from the Bill of Materials and adding comments to components. See Edit or Modify a Bill of Materials for examples of this new functionality.
- If you do not manually define a Scan name on the New Scan dialog, the name of the uploaded artifact is automatically applied as the Scan name.
- Messaging has been improved for cases in which a user attempts to start a scan or add a product after their CodeSentry license has expired or licensed scan limit has been reached.
- Additional information may be displayed in the Scan Status tab. For example, if an analysis is attempted more than one time, the user interface will display an *Analysis Begin Time* and *Analysis End Time* entry for each analysis run associated with the file.
- The Scan Report title page now includes the CodeSentry version used to execute the scan.
- There is a new widget on the CodeSentry CodeSentry Dashboard, **Last Updated**, which indicates the age of the oldest data displayed on the dashboard.
- The CycloneDX export now includes component license information.
- The scan status *Collating Results for Reports* has been renamed *Analyses Completed, Results Not Collated*.

- **API Changes**

- Updates to internal services to improve the responsiveness of API functionality have been introduced in this release.
- There is an updated query for viewing scan status.

- **Bug Fixes**

- This release includes several bug fixes, including:
 - An issue where highlighting in the *Affected Products* section of the N-Day Findings tab was not working as expected, has been fixed. The vendor(s) and version(s) affected by the vulnerability are highlighted in red; unaffected versions are highlighted in green.

- An issue where reported versions of Java components appear to differ from the file name, has been fixed.
- **Documentation Change**
 - There is a new page in the manual describing the procedure for Adding Worker Nodes to on-premise installations.
 - There is a new page in the manual describing CodeSecure's Backup Strategy.
- **Updated Kubernetes**
 - SaaS Kubernetes Cluster upgraded to version 1.23.
- **Updates to Vulnerability Information**
 - CodeSentry 5.0 includes over 9,700 new vulnerabilities and 3,700 new products.
- **Analysis Engine Updates**
 - Ongoing improvements and refinements to the CodeSentry analysis will result in changes to reported components and vulnerabilities compared to previous versions of CodeSentry.

CodeSentry 4.2.3 Release Notes

- **Bug Fixes**
 - This release includes several bug fixes, including:
 - An issue in the Zero-Day Findings section of the Scan Report related to archives scanned with Zero-Day analysis enabled where the *Top 25 CWE Findings* entry in the **Zero-Day Findings** section erroneously reported zero *Instances* for the CWEs that CodeSentry can detect (CWE:89, CWE:78, CWE:416, CWE:798, CWE:119), has been fixed.
 - An issue where skipped targets were not listed on the Scan Status tab, has been fixed. Tabs for each requested analysis type are displayed in the user interface, and these tabs now list skipped files and the reason the files were skipped.
 - Corrected a condition where some *fuzzy* component matches were not being reported.
 - An issue where trying to download an SPDX bill of materials while results were still collating resulting in an error message saying "Unknown Reason" has been fixed. Error messaging has been changed to indicate the reason for the download failing.
 - An issue where special characters were not handled gracefully in SPDX bills of materials, has been fixed.
 - Unpacking archives is now more resilient to temporary network failures.
 - The Scan Report no longer displays multiple CVSS scores for a given component, but instead displays just one CVSS v2.0 score (if it exists) and one v3.0 score (if it exists). The UI will continue to display all CVSS scores for a given component.
 - Several error messages have been made more informative.
 - Fixed a cause of rare scan failures in Security Attributes and shallow Zero-Day scans.
 - An additional issue causing scans to fail sporadically with the error "Failure Description: Failure to analyze", has been fixed.
 - An issue on the New Scan dialog in which application names added in the current user session were not appearing in the autocomplete suggestion list, has been fixed.

- Properties in the expanded rows on the Scan Status tab are now listed in the order that they were updated, except for **Job Id** and **Job Last Updated**, which are always listed last. In addition, users can now see multiple identical properties. For example, if an analysis is attempted more than one time, users will see **Analysis Begin Time** and **Analysis End Time** for each analysis.
- **Updates to Vulnerability Information**
 - CodeSentry 4.2.3 includes over 2,200 new vulnerabilities and 1,200 new products.

CodeSentry 4.2 Release Notes

- **CodeSentry Editions**
 - CodeSentry v4.2 introduces *CodeSentry Editions*, which offer different functionality dependent upon licensed features. Existing customers will be transitioned to the appropriate Edition based on their licensed features. Contact your CodeSecure sales representative for more information on CodeSentry Editions.
- **CodeSentry Dashboard**
 - The user interface now includes the CodeSentry Dashboard which includes a number of widgets with instance-wide information on scans, components, and vulnerabilities (if applicable).
- **Performance and Reliability Enhancements**
 - Overhead associated with processing files has been reduced, which will improve target analysis throughput.
 - N-Day scan reliability has been improved.
- **Component Search**
 - There is a new Components tab on the Summary page. This page lists the complete set of components discovered by all scans performed on your instance, and provides various search options for finding scans which include specific components.
- **Updates to Vulnerability Information**
 - CodeSentry v4.2 includes over 2,300 new vulnerabilities and 3,800 new products.
- **VEX Document Export**
 - **Vulnerability Exploitability eXchange (VEX)** document export is now available for N-Day analyses. You can download VEX documents from the Scan Results: Bill of Materials tab.
- **User Interface Changes**
 - There is a new About CodeSentry page in the user interface which displays information on which CodeSentry Edition your instance is licensed for license expiry date, licensed scan count, and remaining scans.
 - The **Scan Depth** slider has been removed from the New Scan dialog. Deep scans can still be performed via the API.
 - Analysis engine version information has been added to the expanded row details, where applicable, on the Scan Status tab. The new fields are labelled **Carbon Version** and **CodeSentry Version**.
 - Dark mode user preference is now saved between user sessions.
- **Bug Fixes**

- This release includes several bug fixes, including:
 - An issue where hover text on the left navigation bar was blocking user interface controls, has been fixed.
 - An issue causing scans to fail sporadically with the error "Failure Description: Failure to analyze", has been fixed.
 - Upload reliability for slow networks/low throughput, has been improved.
 - An issue where uploads would fail until a user logged out and logged back in, has been corrected.
- **Report change**
 - The *Binary Scan Vulnerability Report* is now called the *Scan Report*.
- **Common Platform Enumeration (CPE) Data Added to CodeSentry Exports**
 - The CPE associated with each component is now included in the CSV, SPDX, and CycloneDX exports.

CodeSentry 4.1.2 Release Notes

- **Updates to CodeSentry Components**
 - No changes to product behavior are expected.
- **Updates to Vulnerability Information**
 - This release includes an updated product database. On-premise users will need to upgrade their installation to v4.1.2 to get the updates. SaaS updates are done automatically (check the version number in the footer of the user interface to verify that your instance is running v4.1.2).
 - CodeSentry v4.1.2 includes over 1,700 new vulnerabilities and 500 new products.

CodeSentry 4.1.1 Release Notes

- **Updates to Vulnerability Information**
 - This release includes an updated product database. On-premise users will need to upgrade their installation to v4.1.1 to get the updates. SaaS updates are done automatically (check the version number in the footer of the user interface to verify that your instance is running v4.1.1).
 - CodeSentry v4.1.1 includes over 3,400 new vulnerabilities and 1,000 new products.

CodeSentry 4.1 Release Notes

- **Scanning Performance Improvements**
 - Fixed an issue in on-premise deployments where the default configuration provided insufficient CPU allocation to the analysis engine.
 - Fixed an issue (primarily for on-premise users) where the first scan submitted to the system would take longer than an hour and sometimes fail.
 - SaaS Kubernetes Cluster upgraded to version 1.21.
 - Added support for JavaScript NPM packages that provide dependencies in a `package-lock.json` or `yarn.lock` file. Detection using manifest files requires submitting whole packages using the appropriate documented file extensions.

- Improved component detection for PE, COFF binaries.
- Increased Linkerd Proxy Timeout for both inbound and outbound traffic.
- **Third-Party Component Updates**
 - Updated a number of open-source components.
- **Improved Version Detection**
 - The accuracy of version detection of open source components found in DLLs has been improved.
- **Bug Fixes** This release includes several bug fixes, including:
 - Fixed a bug introduced in v4.0 where the "retrieve more" text did not display at the end of the applications or scans list in the left navigation menu if more than 50 applications or scans were listed.
 - Fixed incorrect top-level CycloneDX SBOM component type.
- **Report Improvements**
 - Fixed an issue where reports for large scans would not be generated. Additionally, report documentation has been updated to describe report generation limits.
- **GovCloud Support**
 - CodeSentry deployments now can run in AWS GovCloud.
- **Updates to Vulnerability Information**
 - CodeSentry v4.1 includes over 4,700 new vulnerabilities.
- **Documentation Change**
 - CodeSentry performance information has been added to the documentation.

CodeSentry 4.0 Release Notes

- **Increased Language Support**
 - CodeSentry now supports analysis of binaries and components originating from the following source languages:
 - C#
 - Go
 - Java
 - JavaScript
 - Python
- **Expanded Support for Embedded and Mobile Applications**
 - CodeSentry now supports analysis of the following:
 - Android Dex/Odex
 - APK (Android Application Package)
 - ARM64
 - iOS applications (`.ipa` files)

- **Version Detection**
 - Detection of older versions of components has been improved.
- **New Artifact Support**
 - CodeSentry now detects and analyzes the following new artifact types:
 - `.ext2` , `.ext3` , `.fat` , `.mbr` , `.whl` .
 - VMDK filesystem image.
- **New Firmware Analysis Capability**
 - CodeSentry now offers support for firmware binaries in the following formats:
 - Aris
 - base64
 - bFLT
 - Cisco
 - Intel HEX
 - JFFS2
 - Juniper
 - Kosmos
 - romfs
 - SREC-S Record
 - ubifs
 - uBoot
 - wim
 - yaffs2
- **Updates To Vulnerability Information**
 - CodeSentry v4.0 includes over 11,000 new vulnerabilities.
- **On-Premise Installation**
 - The on-premise installation procedure has changed. Gravity has been replaced by Replicated.
- **N-Day Findings Search Enhancement**
 - You can now search via VulnDB ID in addition to CVE ID.
- **User Interface Changes**
 - CodeSentry now includes dark mode.
 - The Cancel Scan button has been relocated on the Scan Status tab.
 - **Zero-Day and N-Day Finding Details** has been split into two sections - N-Day Finding Details and Zero-Day Finding Details.
 - Export processing indicators have been added to communicate that CSV, CDX, or SPDX report export is underway.
 - The Zero-Day Findings tab columns have changed. The `Target` field is gone, and `File path` was moved into the table of warnings.
 - An upload percentage indicator has been added for the original user/browser window in which the upload was started.

- There is a new section in the Detailed Vulnerability Report, N-Day Findings Summary.
- The Bill of Materials section of the **Binary Scan Vulnerability** Report has been reformatted.
- **Documentation Change**
 - Updated API guide with instructions for uploading large artifacts.

CodeSentry 3.1.1 Release Notes

- **Bug Fixes** This release includes several bug fixes, including:
 - Fixed a large memory leak in the CodeSentry strings-based analyzer.
 - The symbols analyzer speed has been increased.
 - Fixed a memory leak in the CodeSentry analyzer controller.

CodeSentry 3.1.0 Release Notes

- **log4j Detection**
 - CodeSentry detects the presence of the **log4j** Java component and associated vulnerabilities. To facilitate the identification of **log4j** , **.jar** files are analyzed, and not unpacked.
- **Software Package Data Exchange (SPDX) bill of materials**
 - An **SPDX bill of materials** is now available for N-Day analyses. You can access this bill of materials through the user interface (from the Scan Results: Bill of Materials tab) or through the API (using the **/export/spdx/** endpoint).

CodeSentry uses the SPDX Tag format from SPDX version 2.2.

- **CycloneDX SBOM**
 - CycloneDX SBOM now includes supplier (vendor) information, and licenses when available.
- **New Scan Type**
 - A Security Attributes analysis that was previously available via the API can now be requested via the UI. This scan type identifies security-relevant properties that may indicate potential weaknesses. Results for Security Attributes analyses appear in the UI and Binary Scan Vulnerability Report.
- **N-Day Scan Depth** N-Day scanning is restricted to shallow analysis depth in the user interface. This limitation may be removed in a future version.
- **Archives**
 - CodeSentry can now handle ISO 9660 disc images (**.iso**), and bare Ext4 (**.ext4**) and SquashFS (**.sqsh**) filesystem images.
- **Terminology Changes**
 - Scan types formerly known as **0-day** have been renamed to **Zero-Day** throughout the product.
 - 'Projects' are now called 'Applications'!
 - 'Applications' are now called 'Scans'!
- **API Changes**

- Submission of new jobs should use `zero-day` instead of `0-day` for the `analyzer_type` (whether they are part of a composite job or not).
 - Jobs that already exist in the database will have their `analyzer_type` changed from `0-day` to `zero-day`. Note that this will reorder the types in a composite job to stay in ASCII order – for example, `0-day, n-day` will become `n-day, zero-day` (not `zero-day, n-day`).
 - The endpoint for accessing CycloneDX results through the API has changed from `/cdx/bom/` to `/export/cdx`.
 - New scan file descriptions submitted via the API are now limited to 200 characters.
- **User Interface Changes**
 - The standalone Bill of Materials in PDF format is no longer available. To retrieve a Bill Of Materials in PDF format, navigate to the Vulnerability Report tab and generate the report.
- **Windows Library Detection**
 - Windows library detection accuracy has been improved.
- **Report and SBOM Generation Improvement**
 - Report and SBOM generation speed for large scans has been increased.
- **On Premise Installation Improvement**
 - Authentication migrations are now automatic.

CodeSentry 3.0.6 Release Notes

- **Bug Fixes** This release includes several bug fixes, including:
 - An issue where a 'Lesser' General Public License displayed in the BoM in the UI as an Unknown license is now fixed.
 - An issue where unknown licenses were displayed in the report with a blank "License" field, is now fixed. Unknown licenses are now marked as "Unknown" in the BoM in the report.
 - An issue where expired mTLS certificates for Linkerd service were causing 503 errors for some AWS deployment users has been fixed. The renewed certificate prevents similar issues for On-Premise users.
 - A known issue where products added via Add Product may not appear when there are too many vulnerabilities now results in a more graceful failure, and includes a job property accessible via the API with a failure message.
 - An issue where scans could get stuck at the state "New Scan (Upload is starting)" has been fixed.
 - An issue where some uploads were failing has been fixed.
 - An issue where an incorrect security score is displayed for some components has been fixed.
 - An issue on the scan status tab with rows not initially displaying when selecting the 'Scanning - Live Update' filter has been fixed.
 - An issue where items temporarily disappeared from an expanded row on the BoM tab while an analysis is running, has been fixed.

CodeSentry 3.0.5 Release Notes

- **Bug Fixes** This release includes several bug fixes, including:
 - An error returned when starting a new scan "Error: creating new scan: Error: connection error" is now fixed.
 - An error when downloading a CycloneDX Software Bill of Materials report of "[object Object]" is now fixed. Crashes of the CycloneDX service should be reduced, and if an error is encountered while downloading a CycloneDX Software Bill of Materials report, it will correctly be reported to the user.
 - An issue with some jobs not reaching the correct state has been fixed. Examples of how this would present itself: some jobs not reaching an end state of "Done", "UploadFailed", or "Skipped", or "Failed", and scans that never complete.
 - CodeSentry version was omitted from the CycloneDX Bill of Materials in certain cases.

- An error "Bill of Materials cannot be returned. OK: Scan is still processing, please try again once the scan has completed" displayed when trying to download CycloneDX report is now fixed.
- An issue with intermittent analysis failures was fixed. A job would fail if there was no vulnerability information returned from the product database.
- An issue with scans becoming increasingly slow or stuck with job(s) stuck in a state other than "Done", "UploadedFailed", "Failed", or "Skipped" was fixed.

CodeSentry 3.0.4 Release Notes

- **Bug Fix** This release fixes a postgres bug that can prevent new projects, applications, and artifacts from being created.

CodeSentry 3.0.3 Release Notes

- **Bug Fix** Correctly handle edge case where Vulnerability database has missing license information.

CodeSentry 3.0.2 Release Notes

- **Documentation Changes** Updated Audit Logging feature documentation.

CodeSentry 3.0.1 Release Notes

- **Gravity Variable Change** An issue with an incorrect gravity variable was fixed.

CodeSentry 3.0.0 Release Notes

- **VulnDB Integration**

CodeSentry is now integrated with VulnDB: a proprietary database of vulnerability information. As a result, there is more detailed vulnerability information available in the *Bill of Materials* and *N-Day Findings* tabs of the Scan Results page, as well as in the Binary Scan Vulnerability Report and through the API.

Some VulnDB vulnerabilities do not have associated CVSS scores. CodeSentry reports the CVSS score for such vulnerabilities as "None", with corresponding severity value "Unassigned".

For more information about VulnDB, see [https://vulndb.cyberiskanalytics.com/](https://vulndb.cyberriskanalytics.com/).

- **Documentation PDFs**

CodeSentry documentation is available in PDF format.

- **Archives**

- CodeSentry can now handle Posix Tar archives (**.pax**) and RAR archives (**.rar**).
- CodeSentry can now handle archives that contain links.
- There is no longer a restriction on the number of files that may be contained in an archive.

- **Description Field for Uploaded Artifacts**

Users can now specify a brief artifact description in the New Scan dialog. This description is displayed on the Scan Results page and in the executive summary of the binary scan vulnerability report.

- **Scan Results page**

- A new **application dashboard** at the top of the Scan Results page replaces the previous badges.
- There is a new Vulnerability Report tab with functionality for customizing and downloading a Binary Scan Vulnerability Report.
- There are several changes to the Bill of Materials tab.
 - The set of download links no longer includes a link for the binary scan vulnerability report: this has been replaced by the new customization tab.
 - The table columns for the component name and version now have headings *Name* and *Version*, respectively (previously "Component Name" and "Component Version").
 - The table column for summarized vulnerability counts now has heading *Vulnerabilities by Severity* (previously "CVSS Distribution") and now includes counts for CVSS *None* scores.
 - There are new table columns *Vendor* and *License*.
 - Search on the *Bill of Materials* tab is now over the *Name* column only.
- Most statistics on the Scan Status tab are now presented as job counts (previously target and analysis counts).
- There are several changes to the N-Day Findings tab.
 - New **Vulnerability ID** and **Vulnerability Title** columns provide the unique identifier and title assigned to the vulnerability by VulnDB.
 - There is now a *CVE ID(s)* column, which lists the identifiers of any CVE entries associated with the vulnerability. This replaces the previous "CVE ID" column. CVE identifiers are specified without the "CVE-" prefix that was previously used. For example, **2011-3045** is now used where **CVE-2011-3045** would have been used previously.
 - The new *Remediation Available* column indicates whether or not VulnDB provides information about remediating the vulnerability.
 - Expanded table entries now contain extensive additional vulnerability information.
- **Binary Scan Vulnerability Report**
 - The contents of the Binary Scan Vulnerability Report are now customizable.
 - There is a new Vulnerability Report tab on the Scan Results page as noted above.
 - The list of artifacts in the Executive Summary includes the user-provided description for each artifact, if any. There is no longer an EIM ID field: you can use the new **description field** to store EIM IDs or other identifiers associated with your artifacts as required.
 - Information about vulnerabilities in the Executive Summary, Bill of Materials, N-Day Findings, and 0-Day and N-Day Finding Details sections now reflects the detail and scoring information provided by VulnDB.

- **Zero-Day Analysis**

The following changes are visible in deployments whose license includes Zero-Day analysis.

- **Scan Depth** now also applies to Zero-Day analysis.
 - The **Deep** setting corresponds to the Zero-Day analysis previously performed in all cases.
 - The new **Shallow** Zero-Day analysis detects only uses of various dangerous functions. Shallow Zero-Day analysis is very fast: a shallow scan with both Zero-Day and N-Day analysis will generally take approximately the same time as a shallow scan with N-Day analysis only.
 - Additional constraints on the type (but not size) of the scanned artifact apply for shallow Zero-Day analyses. See the Available Scan Depths table for details.

The API Guide now includes sample queries for retrieving Zero-Day analysis results.

- **New Scan dialog**

- The new **Scan Depth** setting replaces the previous *N-Day Scan Depth* setting, and controls both Zero-Day and N-Day analysis depth.

- **Menu Panel**

The menu panel is now paginated.

- **API**

The URL for downloading a binary scan vulnerability report now includes an optional query string that specifies the report sections to include. If you specify the URL without a query string, the downloaded report will contain only the title page, table of contents, executive summary, and appendix.

- **Security Attributes Analysis**

The new *security attributes analysis* identifies various security-relevant properties of the executable that do not directly indicate a vulnerability. It is currently available through the API only, and is not available for MacOS binaries or files that are not of a recognized executable type.

- **Audit Log DB API**

CodeSentry now provides programmatic access to audit logs.

- **Bugs**

This release fixes a number of bugs, including the following.

- Closing the browser window while a file is uploading will no longer cause the scan to become stuck in 'Uploading' state. Instead, the scan will transition to 'Upload Failed' state.

- **System Requirements**

For on-premise CodeSentry deployments, disable `firewalld`.

When you are setting up an on-premise installation of CodeSentry, the first machine you install on must be capable of accommodating a minimum CodeSentry deployment. The application can then be scaled up by adding additional nodes. Given this, the minimum system requirements are as follows.

minimum requirements	Cores	RAM	Storage
first machine	24	48 GB	1.1 TB
subsequent machines	7	18 GB	600 GB

CodeSentry 2.1.2 Release Notes

- **Bugs**

This release fixes a regression in the Bill of Materials section of the Binary Scan Vulnerability Report: missing security scores for components are now present.

CodeSentry 2.1.1 Release Notes

Minimum CPU requirements were updated.

- **Bugs**

This release fixes one bug related to a regression in components found during scans.

CodeSentry 2.1 Release Notes

CodeSentry v2.1 includes the following changes and improvements.

- **Archive Types**

CodeSentry can now handle RPM Package Manager packages (`.rpm`).

- **Scan Results Page**

A table pagination bug on the Scan Status tab has been fixed: the table now updates correctly when you use the interface controls to move to the next or previous page, or when you apply a search or status filter.

- **Summary Page**

- Performance for the Summary page has been improved.
- The Applications table can now be sorted by the **Application Name**, **Project Name**, and **Application Created** columns only.

- **Binary Scan Vulnerability Report**

The Binary Scan Vulnerability Report now includes a table of contents that provides a link to the beginning of each section.

- **Scan States**

- There is no longer a **Cancelling** state.
- The heading of the Scan Results page now includes more information for several scan statuses.

- **General**

There are a number of performance improvements and bug fixes in this release.

CodeSentry 2.0 Release Notes

CodeSentry v2.0 includes the following changes and improvements.

- **Archive Types**

CodeSentry can now handle 7z (`.7z`) archives and Microsoft VSIX files (`.vsix`).

- **Directly Add Products To An Application**

If you know that your application includes a specific *product*, you can use the CodeSentry **Direct Add** functionality to explicitly include that product in the set of application components. Any stored information about the product and its vulnerabilities will be added to the set of results for the application.

- New Add Product dialog available from the Scan Results page.
- Direct Add in API.

- **API**

- New **vendor** column available when retrieving component information, such as with **ext_job_components_found** query. The **vendor** column is currently populated only for directly added components, not for components detected by N-Day analysis. This may change in a future version. For more information, see the API Guide.

- **Scan Results page**

- Scan status tab contents are no longer automatically updated. A new refresh button has been added.
- The *Vulnerabilities* tab has been renamed to N-Day Findings.
- The *Vulnerabilities* badge has been renamed to **N-Day Findings**.

- **CycloneDX bill of materials**

A CycloneDX bill of materials (<https://cyclonedx.org>) is now available for N-Day analyses. You can access this bill of materials through the user interface (from the Scan Results: Bill of Materials tab) or through the API (using the **/cdx/bom/** endpoint)

- The download links on the Bill of Materials tab of the Scan Results page are now blue (previously dark grey).
- Changes to scan states related to cancellation.
 - States **Scan Cancelled but Results are Complete** and **Scan Cancelled, Results are Incomplete** have been removed.
 - State **Cancelled** has been added.
 - Scans whose state was previously **Scan Cancelled but Results are Complete** will now have state **Done**.
 - Scans whose state was previously **Scan Cancelled, Results are Incomplete** will now have state **Cancelled**.

- **Zero-Day Analysis Results and Initiation in Web Interface**

The following changes are visible in deployments whose license includes Zero-Day analysis.

- The **Run 0-day Scan** selector has been restored to the New Scan dialog.

At present, Zero-Day analysis can only be performed on files of size 4MiB or less, and cannot be performed on archives. These restrictions may be removed in a future release.

- Scan Results page changes
 - New *0-Day Findings* badge, displayed only when Zero-Day analysis has been performed.
 - New 0-Day Findings tab, available only when Zero-Day analysis has been performed.

- **On-Premise Installation**

- One of the commands involved in performing your own TLS configuration for on-premise CodeSentry installation has changed. The On-Premise Installation Instructions have been updated with the new command.
- We now provide instructions for backing up your on-premise deployment, and for removing unused files to recover disk space.

- **Binary Scan Vulnerability Report**

The Binary Scan Vulnerability Report now includes an appendix describing how scores are calculated and providing supporting information about the various report sections.

- The **Debug Information** window has been replaced, and the formatting has changed.

- When launched from the Bill of Materials tab or N-Day Findings tab, this window is now called **Component Match Details**.

- When launched from the 0-Day Findings Tab, this window is now called **0-Day Finding Details**.

CodeSentry 1.5.4 Release Notes

CodeSentry v1.5.4 includes the following changes and improvements.

- **Combined N-Day/Zero-Day Scans**

Where Zero-Day analysis is licensed, you can perform combined N-Day and Zero-Day scans rather than initiating separate scans to cover each analysis. For more information, see the API Guide.

- **N-Day Scan Depth**

Archives can only be scanned with a shallow analysis depth. This limitation may be removed in a future version.

While this limitation was only placed on scans instantiated via the User Interface, we discourage deep scans of archives via the API. Deep scans that include many targets will not complete in a reasonable amount of time.

- **User Interface Changes**

- **Summary Page**

For performance reasons, the *Applications with Findings* badge box has been removed, and the *Scan Status* and *Pass/Fail* columns have been removed from the applications table. They will be restored in a future release.

- **Bugs**

This release fixes two bugs that caused frequent analysis failures, leading to low availability for analyses.

CodeSentry 1.5.3 Release Notes

CodeSentry v1.5.3 includes the following changes and improvements.

- **Zero-Day analysis capability**

Where licensed, you can perform Zero-Day analyses, currently available only through the CodeSentry API.

- The **Run 0-day Scan** selector has been removed from the New Scan dialog.
- New columns have been added to the Scan Status tab of the Scan Results page.
- Summary information about the scan has been updated to reflect that now each target can have both a Zero-Day analysis and N-Day analysis.

CodeSentry 1.5 Release Notes

CodeSentry v1.5 includes the following changes and improvements.

- **Zero-Day analysis capability**

Where licensed, you can perform Zero-Day analyses through the CodeSentry UI.

- A new **Run 0-day Scan** selector has been added to the New Scan dialog. Enable this selector to perform Zero-Day scanning in addition to the standard ("N-Day") scan.
- A new **Scan Type** column has been added to the Scan Status tab of the Scan Results page.

Zero-Day analysis information is available in the CodeSentry UI *only if there is also an N-Day scan of the same application* (this behavior will change in a future release). For Zero-Day scans initiated through the New Scan dialog there will always be a corresponding N-Day scan.

- Zero-Day analysis results are available in the Binary Scan Vulnerability Report.
- Zero-Day scan status information is available in the **Scan Status** tab of the Scan Results page.

You can use the API to perform a Zero-Day scan in isolation. In this case, you will only be able to obtain the scan status and Binary Scan Vulnerability Report through the API: the Scan Results page will not be available unless there is also an N-Day scan.

- **Binary Scan Vulnerability Report**

The Binary Scan Vulnerability Report has been extended to also provide information about Zero-Day vulnerabilities detected in the project.

- **API**

If Zero-Day analysis is available, you can perform Zero-Day scans through the CodeSentry API.

To support this functionality, the `new_scan` mutation has a new required field: `analyzer_type`. See API Guide: C. Create a Scan for details.

CodeSentry 1.4 Release Notes

CodeSentry v1.4 includes the following changes and improvements.

- **Binary Scan Vulnerability Report**

The Binary Scan Vulnerability Report provides an executive summary with aggregate information about the security of a single project, along with detailed information about all the components detected in the project artifacts and the vulnerabilities associated with each component.

- **Session Timeout Changes**

A session dialog now opens after 5 minutes of user session inactivity. Click the **Refresh** button in the dialog within 30 seconds in order to keep the session open.

- **Archive Types**

CodeSentry can now handle Tar (`.tar` , `.ova`), Xz (`.xz` , `.txz`), Gzip (`.gz` , `.gzip` , `.tgz` , `.tpz`), Xar (`.xar` , `.pkg`), Cpio (`.cpio`), and bzip2 (`.bz2` , `.bzip2` , `.tbz` , `.tbz2`) files in addition to the archive types previously supported.

Dmg (`.dmg`) archives are partially supported: HFS/HFS+ only.

- **Changes to System Requirements**

There are some changes to the CodeSentry system requirements for on-site installation

- Each node in the CodeSentry cluster must have a minimum 400 GB of disk space (previously 120 GB).
- The minimum required total disk space in the cluster is 1TB (previously no total cited).
- Each node in the CodeSentry cluster must have a minimum 6 virtual cores (previously 4)
- The combined number of virtual cores in the CodeSentry cluster must be at least 14 (previously 12).
- We recommend 32 cores for optimal performance.

CodeSentry 1.3 Release Notes

CodeSentry v1.3 includes the following changes and improvements.

- **Archive Types**

- CodeSentry can now handle AR (`.a` , `.ar` , `.deb` , `.lib`), Cab (`.cab` , `.msu`), and Compound (`.msi` , `.msp`) archives in addition to ZIP archives.
 - Note that `.deb` archives are frequently layered `ar/gz/tar` or `ar/xz/tar` . The GZ, XZ, and TAR layers are *not* currently handled - this functionality will be added in a future release.
- A broader range of ZIP file extensions is now accepted: `.zip` , `.jar` , `.ipa` , `.xpi` .
- For more information, see System Requirements: Requirements for Scanned Files.

- **File Size Limits**

There are a number of changes to file size and archive expansion limits.

- Maximum file size limits:
 - Uploaded artifact: 7GB.
 - Archive (whether uploaded directly or extracted from another archive): 7GB.
 - Analysis target (whether uploaded directly or extracted from an archive): 1GB.
- The maximum number of targets in a single artifact is 30,000.
- Archives may not expand to more than 1.5x their size.

CodeSentry 1.2 Release Notes

CodeSentry v.1.2 includes the following changes and improvements.

- **TLS Certificates**

You can provide your own TLS certificates to use with on-premise CodeSentry deployments. See Installation Instructions: TLS Note for details.

- **User Interface**

Performance has been improved for all user interface pages that display information about CodeSentry analyses.

- **Results API**

The structure of the results database has changed. In particular, vulnerabilities are now stored as structured objects. See API Guide: Get API/JSON Results for updated result queries.

- **Bugs**

This release fixes several bugs that caused interruption or impairment to CodeSentry functionality.

CodeSentry 1.1 Release Notes

CodeSentry v1.1 includes the following changes and improvements.

- **Scan Depth** There are two available scan depths: **shallow** and **deep**.
- **Scan Scheduling** Shallow scans and deep scans are managed in separate queues and performed by separate workers, so deep scans cannot block shallow scans.
- **Scan Status Tab** The Scan Status tab of the Scan Results page has undergone several changes.

- Performance has been improved.
- Summary information about the scan is displayed at the top of the tab.
- Table rows can be filtered by status.
- If the status filter is set to **Scanning - Live Update** the information in the Scan Status tab is automatically updated as the scan progresses. For other filter settings the information is not automatically updated: you can view updated information by reloading the tab or switching back and forth between filter settings.

CodeSentry 1.0 Release Notes

Welcome to CodeSentry! This is the first CodeSentry release and provides the core functionality that we will be improving, extending, and supplementing in future releases.

CodeSentry analyzes binaries, detecting the **components** (such as libraries) that have been compiled in. In this release you can:

- **Upload** binaries and archives to be scanned.
- View or download a **Bill of Materials** listing the components that CodeSentry detected.
- Find out which CVE **vulnerabilities** are associated with the detected components.

For a guided introduction to installing and using CodeSentry, see the manual's Getting Started section.

The Details

- **System Requirements:** CodeSentry on-site installation uses Gravity; consequently the operating system and hardware requirements for CodeSentry are closely related to those for Gravity as described below.
 - **OPERATING SYSTEM:** Linux only. Distributions officially supported by Gravity are listed at <https://gravitational.com/gravity/docs/requirements/>.
 - **MEMORY:** Every node in the CodeSentry cluster must have a minimum 24 GB of memory.
 - **DISK:** Every node in the CodeSentry cluster must have a minimum 125 GB of disk space. The master does *not* require additional disk space. A separate disk for etcd is *not* required. High-IOPS disks are recommended.
 - **CPU:** Every node in the CodeSentry cluster must have a minimum 4 virtual cores. The combined number of virtual cores in the cluster must be at least 12.
 - Otherwise, hardware requirements are as described for Gravity at <https://gravitational.com/gravity/docs/requirements/>.
- **Input File Types:** binary or archive files as shown in the following table.
 - The maximum file size, including for archives and files extracted from archives, is 1.5 GB.
 - An archive can contain at most 1000 files and folders (including those inside contained archives).

Analyzable Binary File Type	Typical File Extension	Archive File Type	Required File Extension
Linux executable	<i>none</i>	ZIP	.zip
Linux shared library	.so		
Windows dynamic linked library	.dll		
Windows executable	.exe		

- **Analyzed Binaries**
 - **Platform:** Windows, Linux, MacOS. Scans at *shallow* depth can be performed on binaries for any of these platforms; *average* and *deep* scans can be performed on Windows and Linux binaries only.
 - **Architecture:** *shallow* scans can be performed on binaries with any architecture, *average* and *deep* scans can be performed on x86 and x64 binaries only.
 - **Size:** *shallow* scans have no size restrictions other than the global 1.5 GB file size limit; *average* scans additionally require that the code section be 40 MB or smaller; *deep* scans that the code section be 10 MB or smaller.

What's Coming Up

Features to be added in future releases include:

- **SaaS delivery** for organizations who don't want to manage their own CodeSentry clusters.
- **Analysis for more kinds of binaries:** more platforms, more architectures, bigger code sections.
- **RBAC** (role-based access control).

We Welcome Your Feedback!

Please contact us at support@codesecure.com with any feature requests, support questions, bug reports, or anything else you'd like us to know.
