









































# Compare Vigiles Security Monitoring & Management Versions

## Compare Vigiles Versions

	<b>BASIC</b> Free version providing CVE monitoring for a single component list	<b>PLUS</b> Basic's CVE monitoring upgraded to unlimited component lists, plus collaboration tools for CVE triage and mitigation, advanced filtering, detailed notifications, and advanced reporting tools	<b>PRIME</b> All features of Basic and Plus, along with unique Patch Notification & Management features, links to Linux kernel patches based on identified CVEs, advanced CVE filtering and fixed version notification for OSS
<b>Duration/Term</b>	Free	Annual Subscription	Annual Subscription
<b>CVEs affecting your software components</b> List of the Common Vulnerabilities & Exposures (CVEs) specific to your software components in your loaded manifest	Detailed	Detailed	Detailed
<b>Push Notifications of vulnerabilities</b> Notification of new CVEs that are associated with the software components in your loaded manifest	Summary	Detailed	Detailed
<b>Track multiple Software Bill of Materials (BOMs)/manifests</b> Ability to load product manifests listing your software components and versions	Limited to 1	Unlimited per product family	Unlimited per product family
<b>On-demand CVE report generation via web</b> Notifications of vulnerabilities available on-demand in multiple formats			
<b>On-demand CVE report generation via command line</b> Notifications of vulnerabilities available on-demand in multiple formats	Summary	Detailed	Detailed
<b>CVE summary by severity, status and software package</b> View summary counts of Common Vulnerabilities & Exposures by the			

<p>severity score derived by the Common Vulnerability Scoring System as listed in the National Vulnerability Database (NVD) maintained by the US Government's National Institute of Standards and Technology. Also includes ability to view CVEs by the status of resolution in your manifest and by those specific to your software components.</p>			
<p><b>Build system support: Yocto, Buildroot and Timesys Factory</b>          Ability to upload Yocto manifest (generated by meta-timesys), Buildroot manifest.csv, or Factory workorder from command-line and web for CVE scanning</p>			
<p><b>Support for custom component lists (CSV format)</b>          Ability to upload open source component lists used by applications and BSPs for CVE scanning</p>			
<p><b>Upload your Software BOM or create one using Web wizard</b>          Upload open source component lists used by applications and BSPs for CVE scanning. Also includes ability to create custom software component lists in order to generate a CVE report and receive security notifications independently of any build engine.</p>			
<p><b>Software License Information (Yocto and Buildroot only)</b>          View summary of CVEs and license stats for each package.</p>			
<p><b>Filter based on Component or Status</b>          Filter CVEs by those specific to your software components or by the status of resolution in your manifest.</p>			
<p><b>CVE search tool for Timesys curated CVE database</b>          Ability to search for CVEs by package name and version, or by ID</p>			
<p><b>CVE report history with CVE trend plot</b>          View previously generated reports and track how threats in your build have changed over time</p>			

<p><b>CVE report sharing</b> Share a view-only version of the latest CVE report via a link. This is particularly useful when you want to quickly share a report with others who might not be on the same team.</p>			
<p><b>Early CVE notification</b> Notification of newly discovered CVEs that are not yet in the NVD data base</p>			
<p><b>Team sharing and CVE mitigation collaboration tools</b> Vulnerability management workspace and tools for you and your team members to comment, annotate, and collaborate on triage and mitigation of each vulnerability listed in your manifests.</p>			
<p><b>Continuously track specific issues and CVE status changes</b> Continuous tracking of vulnerabilities based on resolution status for your manifests.</p>			
<p><b>Whitelist already reviewed CVEs to streamline reviews</b> Ability to hide CVEs that are already being addressed so as to simplify reports, collaboration and mitigation</p>			
<p><b>Filter reports by severity (CVSS) score or attack vector</b> Filter Common Vulnerabilities &amp; Exposures by the severity score derived by the Common Vulnerability Scoring System as listed in the National Vulnerability Database (NVD) maintained by the US Government's National Institute of Standards and Technology or by the technique by means of which unauthorized access can be gained to a device or a network. Also includes ability to view CVEs by the status of resolution in your manifest.</p>			

<p><b>Software BOM/Manifest editor and revision management</b>  Add packages, modify package names or versions for Buildroot, CSV, and Yocto SBOMs/manifests, and modify licenses for Buildroot and Yocto SBOMs/manifests. Saving creates new SBOM/manifest in the same product as the previous version with the changes applied.</p>			
<p><b>Download reports in different formats</b>  Ability to export reports in a variety of formats</p>			
<p><b>Comparison of changes between builds/releases (SBOM/manifest difference)</b>  Quickly generate reports and bulletins to document security issues and vulnerability status on releases for submission to customers and regulatory authorities.</p>			
<p><b>Comparison of reports for new and changed CVEs</b>  Comparison of any two scans to view new, removed, and status changed CVEs</p>			
<p><b>Custom vulnerability score/prioritization and filtering</b>  Assign a custom severity or priority value to each CVE (0.0 to 10.0). Sort and filter based on the custom score, and easily prioritize CVEs based on custom metrics.</p>			
<p><b>Reference links to available patches, mitigation and exploits</b>  Links to the available patch, workarounds for mitigation when a patch is not available, and for recreating the CVE exploit for testing</p>			
<p><b>Link to mainline kernel fix commit for Linux kernel CVEs</b>  A direct link to the CVE fix in the mainline kernel</p>			
<p><b>Minimum kernel version with a fix for a kernel CVE</b>  Identification of the minimum version of a kernel with the CVE fix</p>			
<p><b>Filter reports based on kernel and U-Boot configuration</b>  Ability to filter vulnerabilities based</p>			

on the kernel configuration and U-Boot configuration in your loaded product manifest

**Suggested fix for OSS CVE remediation**

Identifies a version of software where the CVE is fixed and/or provides links to user space patches where available



**Access to free Vigiles Quick Start Education Program**

A complimentary service for Vigiles customers and Vigiles Prime trial users that gets your vulnerability management process up and running quickly

