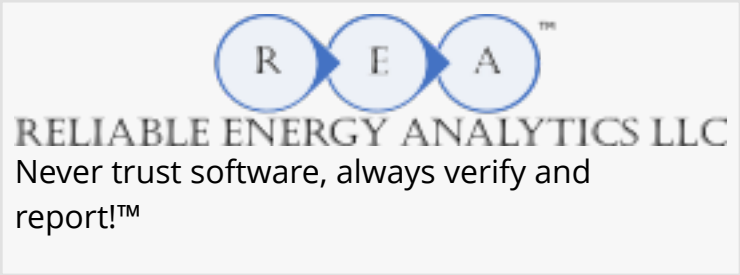
SAG-PM™ Version 1.1.7 Implements Software Rapid Risk Assessment™ (SRRA ™) Method

The Software Rapid Risk Assessment™ methods (SSRA™) in SAG-PM™ helps consumers identify software risks in seconds, when new vulnerabilities are announced



WESTFIELD, MA, USA, January 11, 2022 /EINPresswire.com/ -- Reliable Energy Analytics, LLC (REA™) has been at the forefront of operationalizing Software Bill of Materials (SBOM) to empower software consumers to efficiently identify and manage software risks within installed software products, since 2018. The Software Assurance Guardian™ (SAG™) Point Man™ (SAG-PM™) version 1.1.7 release is the most advanced commercial platform available to perform Software Rapid Risk Assessment™ (SRRA™) methods based on the open-source, free to use, SBOM Vulnerability Disclosure Report (VDR) XML schema, version 1.1.7.

> The SRRA™ methods implemented in SAG-PM™ will help software consumers protect themselves with a rapid response when the next dangerous software vulnerability, i.e., Log4j is announced"
>
> *Joanne Brooks, REA Co-Founder*

The May 12, 2021, Cybersecurity Executive Order, 14028, which takes effect in August 2022, requires software vendors to provide Federal Agencies with an SBOM and notification of vulnerabilities. Federal agencies use the SBOM and VDR as part of a risk assessment process defined by NIST in SP 800-161 Appendix F. Federal agencies, and other software consumers use SAG-PM™ to automate software risk assessments, determining software risks within installed software products within seconds using the SRRA™ methods implemented in SAG-PM™.

The Log4j vulnerability clearly shows that current methods for analyzing software risk are inefficient, slow, and error-prone, leaving software consumers at risk to cyber-attacks from new vulnerabilities for possibly weeks, as this video from Ralph Langner of Langner Group so eloquently articulates. The Software Rapid Risk Assessment™ methods (SSRA™) implemented in SAG-PM™ helps consumers identify software risks in seconds, when new vulnerabilities are announced, addressing concerns and issues raised in the Langner video.

The SRRA™ method requires software vendors to issue both an SBOM and VDR simultaneously upon product release and continuously monitor for new vulnerabilities that may introduce

cybersecurity risks in their products. The software vendor updates their SBOM VDR's as soon as possible after a vulnerability has been reported, to notify customers of any risk in their products from the newly reported vulnerabilities. Software customers use this vendor supplied SBOM and VDR to automate risk assessments using the SRRA™ process implemented in SAG-PM™ to determine risks in seconds, as compared to the manual use of "Security Bulletins", which require cybersecurity professionals to manually read each vendors proprietary security bulletin. SRRA™ methods enable software consumers to initiate a rapid response to new cybersecurity risks, minimizing the amount of time a consumer may be vulnerable to cyber criminals acting to exploit the new vulnerabilities. The SRRA™ methods significantly reduce the amount of time a cyber criminal has to carry out their nefarious acts and provides customers with a rapid response capability, that is not possible with the existing manual Security Bulletin methods that are prevalent today.

The following features describe the open source SBOM VDR and the benefits available from using REA's SRRA™ methods implemented in SAG-PM™ Version 1.1.7, available now from REA™.

- Timing: A SBOM VDR is issued whenever an SBOM is distributed to a software customer
- Update Frequency: An SBOM VDR is updated when a new exploitable vulnerability is confirmed by a vendor and/or when a VEX of CVE is issued
- Recipient: Parties with an NTIA compliant (minimum elements) SBOM for an installed software product that may be exploitable by a newly reported vulnerability (CVE ID)
- Reporter: Software Vendor
- VDR Medium: Electronic XML format communicated to customers, usually via file download from a customer access-controlled portal, typically not publicly available
- Expected Response: Recipient implements automated process implemented in SAG-PM™ Version 1.1.7 to retrieve and process SBOM VDR artifacts when SBOM is initially released and whenever a new vulnerability is confirmed by a software vendor. Take appropriate actions based on a risk priority strategy
- Predominantly an automated process with some manual involvement i.e., determining steps to plan and implement mitigations
- SBOM VDR is an open-source, free to use electronic format for vulnerability reporting on SBOM components, providing considerable benefits to improve risk assessment response time, if broad vendor adoption is achieved
- SRRA™ methods are designed to provide software consumers with automated and improved risk assessments as an alternative to manual Security Bulletin reviews
- Implements rapid risk assessment flags to identify Unresolved Vulnerabilities at the SBOM (product) level and Exploitability at the SBOM component level, as part of the SRRA™ method
- Discloses vulnerabilities and vendor findings at an SBOM component level within a product SBOM

Dick Brooks
Reliable Energy Analytics LLC
+1 978-696-1788

email us here