Updated Open Source SBOM Vulnerability Disclosure Report Format for Rapid Risk Assessment and Response

The free to use, open-source SBOM Vulnerability Disclosure Report (VDR) in XML format released with new, easy to use features indicating exploitability risks

WESTFIELD, MA, USA, December 27, 2021 /EINPresswire.com/ -- Reliable Energy Analytics, LLC (REA ™) announces updates to the open-source, free to use, SBOM Vulnerability Disclosure Report (VDR) in XML format, with new features designed to help customers quickly assess risk, based on the contents of a Software Bill of Materials (SBOM), when new vulnerabilities are reported enabling a rapid mitigation response. Two new elements have been added to achieve these efficiencies:

SAG Logo

- A flag indicating the presence of "Unresolved Vulnerabilities" that exist within an SBOM, and
- An "Exploitable" flag that appears with each reported CVE to indicate whether the CVE is expoEitable, as determined by the software vendor, as of the date/time of a Vulnerability Disclosure Report release.

> Software customers are subjected to slow, manual processes reading vendor security bulletins to determine risks and mitigations when a new vulnerability is reported; a more effective solution exists."
>
> *Dick Brooks*

Software vendors provide consumers with an SBOM document and an associated Vulnerability Disclosure Report (VDR) that is specific to the SBOM that describes a software product's components. Software vendors update their VDR documents when new vulnerabilities are reported, informing customers of a change in status. Software consumers can automate the processing of vendor supplied VDR's as part of a rapid risk assessment and response, whenever a new software vulnerability is reported. This eliminates the slow, error prone, manual processing that occurs today requiring security professionals to locate and read each software vendor

security bulletin for products installed in their ecosystem to determine if any vulnerabilities exist

and must be mitigated. This manual process is quite tedious, slow and error prone due to the level of manual effort that is required to read each vendor's proprietary security bulletin, slowing response time considerably, giving hackers a time advantage to inflict damage on vulnerable sites.

The open-source, free to use Vulnerability Disclosure Report (VDR) produced by REA provides software consumers the ability to rapidly conduct risk assessments on installed software and implement rapid response measures, based on risk priorities. An automated risk assessment using an XML based SBOM VDR can reduce a software consumers exposure to risks from days to minutes when new vulnerabilities are reported.

Version 1.1.7 of the open-source Vulnerability Disclosure Report XML schema and an example VDR are available online:

VDR XML Schema:
https://raw.githubusercontent.com/rjb4standards/REA-Products/master/SAGVulnDisclosure.xsd

VDR Sample:
https://raw.githubusercontent.com/rjb4standards/REA-Products/master/SAGVulnDisclosureSAMPLE.xml

Never trust software, always verify and report! ™

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

This press release can be viewed online at: https://www.einpresswire.com/article/559309448