Vulnerability-Exploitability eXchange (VEX) – An Overview
September 27, 2021

VEX stands for "Vulnerability Exploitability eXchange." The VEX concept and format were developed as part of the National Telecommunications and Information Administration (NTIA) Multistakeholder Process for Software Component Transparency. While the VEX concept was developed to fill a particular need regarding use of software bills of materials (SBOMs), VEX is not limited to use with SBOMs or necessarily expected to be included in the SBOM itself.

The primary use cases for VEX are to provide users (e.g., operators, developers, and services providers) additional information on whether a product is impacted by a specific vulnerability in an included component and, if affected, whether there are actions recommended to remediate. In many cases , a vulnerability in an upstream component will not be "exploitable" in the final product for various reasons (e.g., the affected code is not loaded by the compiler, or some inline protections exist elsewhere in the software).

To reduce effort spent by users investigating non-exploitable vulnerabilities that don't affect a software product, suppliers can issue a VEX. A VEX is an assertion about the status of a vulnerability in specific products. The status can be:

- Not affected – No remediation is required regarding this vulnerability.
- Affected – Actions are recommended to remediate or address this vulnerability.
- Fixed – Represents that these product versions contain a fix for the vulnerability.
- Under Investigation – It is not yet known whether these product versions are affected by the vulnerability. An update will be provided in a later release.

While suppliers could notify users of a non-exploitable vulnerability by email or any other means, a VEX is machine-readable. Machine-readability enables automation and supports integration into broader tooling and processes. Users can integrate component data from SBOMs with vulnerability status information from VEXes to provide an up-to-date view of the status of vulnerabilities. This will likely allow users to take a much more targeted approach to finding and remediating vulnerabilities in their software. A single VEX can convey information about more than one vulnerability in a product, or in multiple products. VEXes will be published by the software supplier, but can also be authored by third parties; users will determine how to use this data.

VEX has been implemented as a profile in the Common Security Advisory Framework (CSAF).[1] CSAF is a standard for machine readable security advisories developed by the OASIS Open CSAF Technical Committee.[2] VEX, as defined by CSAF, can also provide rich information, such as remediation, workarounds, restart/downtime required, scores, and risks that can be provided by vendors, systems integrators, and operators. VEX can also be implemented in other standards or frameworks.

---

[1] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=csaf.
[2] https://github.com/oasis-tcs/csaf/blob/master/csaf_2.0/prose/csaf-v2-editor-draft.md. The VEX profile is at https://docs.oasis-open.org/csaf/csaf/v2.0/csd01/csaf-v2.0-csd01.html#45-profile-5-vex