When to Issue VEX Information

Publication date: November 2023

Introduction

"The goal of Vulnerability Exploitability eXchange (VEX) is to allow a software supplier or other parties to assert the exploitability status of specific vulnerabilities in a particular product or set of products." Issuing VEX information allows developers, suppliers, and others to provide information in a human-readable and machine-comprehensible format, regardless of whether or not software is affected by a specific vulnerability. This allows downstream users to make their own assessments of the risks associated with the vulnerability.

This document seeks to explain the circumstances and events that could lead an entity to issue VEX information and describes the entities that create or consume VEX information. Whether, and when, to issue VEX information is a business decision for most suppliers and possibly a more individual decision for independent open source developers. This document identifies factors that influence the decision.

For background information on VEX, including definitions of VEX data elements and other terminology used in this document, see ***Minimum Requirements for Vulnerability Exploitability eXchange (VEX),***[1] ***Vulnerability Exploitability eXchange (VEX) - Status Justifications,***[2] and ***Vulnerability Exploitability eXchange (VEX) - Use Cases.***[3]

[1] CISA. Minimum Requirements for Vulnerability Exploitability eXchange (VEX). Apri 21, 2023. https://www.cisa.gov/resources-tools/resources/minimum-requirements-vulnerability-exploitability-exchange-vex.

[2] CISA. Vulnerability Exploitability eXchange (VEX) Status Justification Document. June 1, 2022. https://www.cisa.gov/resources-tools/resources/vulnerability-exploitability-exchange-vex-status-justification-document-june-2022.

[3] CISA. Vulnerability Exploitability eXchange (VEX) Use Case Document. April 1, 2022. https://www.cisa.gov/resources-tools/resources/vulnerability-exploitability-exchange-vex-use-case-document-april-2022.

Disclaimer: This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.cisa.gov/tlp/.

Who issues VEX information

Various roles may issue VEX information. This section offers some common examples, but it is not meant to be an exhaustive or limiting set.

Supplier

A supplier is an entity that provides a particular product, software package, library, or component. A supplier could be the original developer of the software, a downstream commercial user, or a third party that repackages the software as a component or dependency of another product. Examples of suppliers include individual software developers, commercial software or device producers, and Linux distributions. Suppliers can issue VEX information to inform their users or customers about the status of a vulnerability in a given product.

Open-source software

In the context of open source software, active developers, maintainers, or project members are examples of suppliers who could provide VEX information. If such roles do not exist, downstream users or community members could provide VEX information. Unmaintained software carries a variety of security and development risks beyond the availability of VEX information.

Researcher

A researcher or finder is an individual or organization that conducts security research or similar assessments and discovers potential vulnerabilities. Examples of this would be individual security researchers or academics, professional bug bounty hunters, or commercial security companies. Researchers could use VEX to report vulnerabilities to suppliers or to publish the status of their findings. Depending on the researcher’s visibility and access to the software, their VEX information may be different than VEX information from suppliers.

Vulnerability coordinator

A vulnerability coordinator is not directly involved in the production of software and assists suppliers, researchers, and others to disclose vulnerabilities in a way that minimizes overall risk. Examples include publicly funded teams like CISA and JPCERT/CC. Commercial bug bounty platforms can also act as coordinators. Coordinators could issue VEX information to provide the status of cases they coordinate. Depending on the coordinator’s visibility and access to the software, their VEX information may be different than VEX information from suppliers.

Vulnerability detection and management

Vulnerability detection and management tools are designed to detect, manage, and report on vulnerabilities. Examples include proprietary or open source vulnerability scanners, software composition analysis (SCA), binary analysis, Application Security Posture Management (ASPM), penetration testing, and security information and event management (SIEM) systems. Such tools may consume or produce VEX information. To reduce false positives, these tools should sufficiently validate the accuracy of VEX information, involving human analysts when necessary.

Other parties

Other parties that may issue VEX information include any entity that might assume responsibility for testing the security of particular software. Examples include regulators, reviewers, service providers, sophisticated software users, auditors, software and technology distributors, and contract software support organizations.

When VEX information could be issued

Various events can drive the issuance of VEX information. The decisions and timing around providing VEX information are primarily business decisions and are not determined by a strict protocol. Common examples are described in this section. These examples are not intended to be comprehensive and are not organized in any specific way. These examples do not limit the events or time frames that can influence the issuance of VEX information.

Upstream vulnerability discovered

As new vulnerabilities are discovered and disclosed, it is common for users or customers to ask for status updates. Issuing VEX information allows users, customers, and the public (if desired) to see the current status and should reduce the number of questions about the vulnerability.

In the course of vulnerability management or other security monitoring activities, a supplier becomes aware of a newly discovered vulnerability that affects an upstream component used by one or more of the supplier’s products. While many upstream component vulnerabilities are not exploitable in downstream products, it is natural to assume that the presence of the vulnerable software or component implies risk, especially when the vulnerability is in a known component listed in a software bill of materials (SBOM).

When this happens, users will attempt to determine to what extent they are affected by the vulnerability. It is common for users to contact the supplier directly, placing a burden on the supplier's communications, support, and cybersecurity teams. By issuing VEX information, the supplier can reduce support calls and communications for incident response teams. As the supplier refines its understanding of the vulnerability, the supplier should update or issue additional VEX information. A vulnerability response program using VEX should provide uniform, up to date, and timely information to help users and suppliers manage their cybersecurity response.

Significant public attention

When a vulnerability is "in the news" (see Figure 1Figure 1) and receiving significant public attention—often in the case of "zero-day," other surprising public disclosure, or reports of active exploitation—it is imperative to provide status and mitigation information using VEX. Users, customers, and the public can access VEX information to obtain the latest vulnerability and exploitability information about the newly disclosed vulnerability. Even when suppliers are also surprised by the disclosure, they can use VEX to convey status information, including an initial "under_investigation." Other parties can also issue VEX information. For example, a researcher or analyst could confirm exploitability for certain products or components.

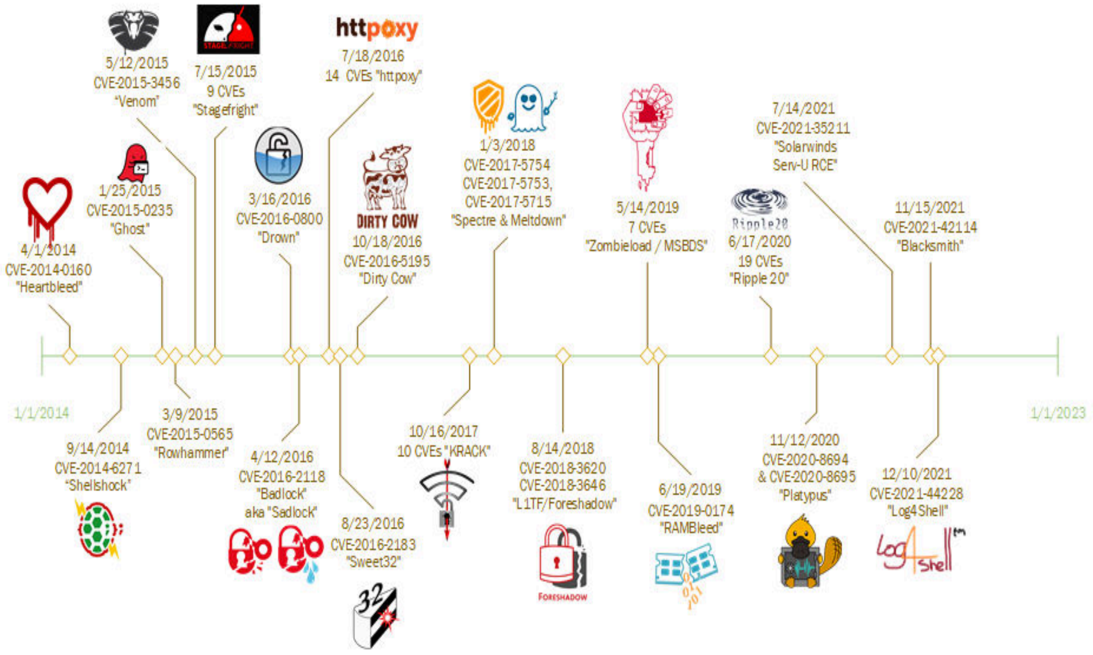

Figure 1: Timeline of named vulnerabilities

Active exploitation

When determining what vulnerabilities can have the most significant impact on the software supply chain, organizations should prioritize vulnerabilities causing immediate harm based on current adversarial activity. VEX "affected" status means that a vulnerability is exploitable, subject to a variety of circumstances. VEX does not specifically describe threat or the degree to which a vulnerability is being exploited, however, such information could be included in the “action_statement” field. Timeliness of notification when considering actively exploited vulnerabilities is vital. This will ensure organizations that consume the software product or component in question are equipped with the necessary information to limit their likelihood of compromise during the time in which the product or underlying components are actively targeted by malicious actors.

There are a variety of public and proprietary sources that organizations may use to determine what known vulnerabilities are being actively exploited in the wild. For example, CISA maintains a publicly available database of exploited vulnerabilities in the Known Exploited Vulnerability (KEV) catalog.[4]

Status changes

In general, VEX issuers are expected to communicate any changes in status. Ideally, when a new vulnerability is disclosed, an “under_investigation” status should be issued. When the investigation has concluded, status should be updated, for example, noting that the product is “affected” or “not_affected.”

VEX information includes timestamps to indicate when the information was first issued and most recently updated. By updating a timestamp but not changing status or other information, a VEX issuer can reaffirm that the current status remains accurate at the present time.

In addition to changes in vulnerability status, VEX can also convey changes to remediation actions (“action_statement”) and further details about “not_affected” status (“impact_statement”).

Coordinated vulnerability disclosure

Coordinated vulnerability disclosure (CVD) and VEX are independent concepts and VEX is neither required by CVD nor does VEX affect CVD. VEX can be used during CVD whenever parties want to convey vulnerability status. For example, a researcher can use VEX as part of a private vulnerability report to a supplier or a supplier can use VEX to privately inform other suppliers. As covered elsewhere, VEX can be used in published vulnerability advisories.

[4] CISA. Known Exploited Vulnerabilities Catalogue. October 10, 2023. https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Legal requirements

There may be legal requirements that create an obligation to issue VEX information. Contract terms could require that a supplier provides VEX information. Industries or sectors could develop guidance about using VEX. Governments could require the use of VEX, for example, in safety-regulated sectors.

Discussion

While not strictly required for decisions to issue VEX information, the following sections provide additional guidance that may be important in deciding when to issue VEX information.

Tools and automation

To work well at scale, VEX will require automation and tools that support the ecosystem. In general, such tools can be grouped into the following three functional categories:

1. Tools that support the creation and maintenance of VEX information
2. Tools that support the consumption of VEX information, also including automated response tools
3. Tools that provide distribution or retrieval methods for VEX information

Different VEX implementations provide these functions within their ecosystem. Interoperability will be important as VEX concepts and implementations develop to support automation and VEX users choose the most appropriate tools for their ecosystems.

In general, the cost of tool creation, communication, and consumption can be reduced dramatically through automation. Nevertheless, some parts, e.g., the analysis of whether the product is affected, might still need human interaction and will therefore be hard to automate. Also, the unique identification of products and correlation against existing inventories are difficult problems to solve at scale, as long as there is a lack of consensus around a global software identification system.

Software supply chain considerations

Supply chains and dependency relationships influence when to issue and how to use VEX information. Status inheritance

VEX information conveys data to VEX consumers who are often developers or suppliers. As a warning, VEX consumers should carefully evaluate if it is valid to inherit status from upstream components. Strictly speaking, consumers should not assume the status of an upstream component applies to a product that uses the component. Each component or product throughout a supply chain may require an independent VEX evaluation.

In certain cases, and with due consideration, a VEX consumer may assume the VEX status of an upstream component can be inherited downstream. For example, a VEX status of “not_affected” with justification “component_not_present” or “vulnerable_code_not_present” could be inherited downstream, unless the vulnerable code is re-introduced elsewhere downstream.

Multiple supply chain paths

VEX consumers should evaluate all supply chain paths and deconflict VEX information for multiple occurrences of the same upstream component. For example, the same upstream component may be used by multiple intermediate components and appear in multiple supply chain paths. To comprehensively evaluate supply chain paths, all VEX information needs to be provided and collected. Accurate SBOM information is important in understanding supply chain paths. VEX authors should consider how best to provide up to date VEX information to VEX consumers.

Trust in VEX information

VEX conveys assertions from the author. The downstream consumer of this information chooses the level of trust and confidence to place in this information. VEX information itself does not convey trust between VEX authors and consumers. Digitally signing VEX information is recommended to support trust in the origin and integrity of the information. Authors and consumers have different types of trust relationships and varying requirements to understand the pedigree and provenance of VEX information. VEX consumers may choose to apply additional validation of VEX information and authors, based on the consumer’s regulatory, compliance, or risk management obligations.

It is common and reasonable to treat VEX information from a supplier as authoritative for components and products produced or maintained by that supplier. VEX, however, does not dictate this or any trust policy. VEX includes authorship (the “author” field) and VEX consumers are free to determine their trust in sources of VEX information.

Open-source software

Regarding VEX, both open source and proprietary software components should operate similarly. For downstream consumers and suppliers of open source components, there are nuances around how upstream open source communities manage vulnerabilities.

For the purposes of VEX and the scope of this document, there are no meaningful differences between open source and proprietary software. Open source components are widely used in proprietary software products and open source suppliers can and should issue VEX information. Open source components can be used in different ways and independent VEX information should be issued for each use of any upstream component. However, it is important to acknowledge that many open source projects and maintainers do not have the resources to create and update VEX information. Similar to proprietary software, no user of open source software should assume that the absence of VEX, or other vulnerability information, implies a lack of risk.

Acknowledgements

This document was a product of the VEX Working Group, which grew out of the NTIA Multistakeholder Process and the Framing Working Group, initially beginning work in 2020. That work continued into 2023, facilitated by CISA. Participants included:

Aditi Sharma, Dell Technologies
Adolfo García Veytia, Chainguard
Adrian Diglio, Microsoft
Allan Friedman, CISA
Amy Villaseñor, Manifest
Art Manion, ANALYGENCE Labs
Bob Haack, Johnson and Johnson
Brandon Lum, Google
Bruce Lowenthal, Oracle
Cassie Crossley, Schneider Electric
Charlie Hart, Hitachi America Ltd.
Charlie Jones, ReversingLabs
Chris Campbell, SolarWinds
Chris Gregoire, Boston Scientific
Christopher “CRob” Robinson, Intel Corporation and OpenSSF
Craig Trump, Hewlett Packard Enterprise
Curtis Yanko, Grammatech
Derek Garcia, Rochester Institute of Technology
Dmitry Raidman, Cybeats
Duncan Sparrell, sFractal Consulting
Ed Heierman, Abbott
Jay White, Microsoft
Jeremiah Stoddard, INL

Jim Jacobson, Siemens Healthineers
John Cavanaugh, Internet Infrastructure Services Corp.
Josh Bressers, Anchore
Joyabrata Ghosh, Elektrobit
Justin Murphy, CISA
Megan Doscher, CISA
Mike O'Connor, HPE
Nicholas Vidovich, Finite State
Nisha Kumar, Oracle
Oscar van der Meer, MergeBase.com
Peter Lund, NetRise
Rene Pluis, Philips
Ricardo Reyes, Tidelift Inc.
Robert Smigielski, B.Braun Medical Inc.
Thomas Schmidt, Federal Office for Information Security (BSI) Germany
Tom Alrich, Tom Alrich LLC
Victoria Ontiveros, CISA
Yotam Perkal, Rezilion