

OpenVEX

Dan Lorenc

Why OpenVEX?

- Let's start with why VEX
 - Lots of reasons, but we care about vulnerability management and false positives
 - Let's use this example:
 - `grype cgr.dev/chainguard/node`

Follow along at home!

```
dlorenc@MacBook-Pro os % gype cgr.dev/chainguard/node
✓ Vulnerability DB [no update available]
New version of gype is available: 0.58.0 (currently running: 0.56.0)
✓ Loaded image
✓ Parsed image
✓ Cataloged packages [273 packages]
✓ Scanned image [1 vulnerabilities]
```

NAME	INSTALLED	FIXED-IN	TYPE	VULNERABILITY	SEVERITY
events	3.3.0		npm	CVE-2018-25076	Critical

Let's see what that CVE is


CVE-2018-25076 Detail

Description

A vulnerability classified as critical was found in Events Extension. Affected by this vulnerability is the function getRandomFeaturedEventByDate/getUpcomingFeaturedEventsInCategoriesWithSubcategories/recacheEvent/searchResults of the file classes/events.php. The manipulation leads to sql injection. The name of the patch is 11169e48ab1249109485fdb1e0c9fca3d25ba01d. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-218395.


Base Score: **9.8 CRITICAL**


Link to the patch


 [timbuckingham](#) / [bigtree-events](#) Public

[Code](#) [Issues](#) 1 [Pull requests](#) [Actions](#) [Projects](#) [Wiki](#) [Security](#)

Added methods for getting a page of upcoming events, fixed SQL inject...
...ion in searches

 [release](#)

 **timbuckingham** committed on Mar 19, 2018

 Showing 2 **changed** files with **107 additions** and **11 deletions**.

Huh, that looks like PHP...

timbuckingham / bigtree-events Public

Watch 1










<> Code Issues 1 Pull requests Actions Projects Wiki Security Insights

release 1 branch 0 tags

Go to file

Add file

<> Code

 timbuckingham Removing the "Today" button. Fixing PHP 7.2 warning. 0c36a7e on Aug 3, 2018 🕒 13 commits
 ajax Removing the "Today" button. Fixing PHP 7.2 warning. 5 years ago
 classes Added methods for getting a page of upcoming events, fixed SQL inj... 5 years ago
 css Fixed missing pagination arrows on Calendar 8 years ago
 field-types/date-chooser Switching to full PHP tags everywhere, adding in support for 4.2.17's... 6 years ago
 js Switching to full PHP tags everywhere, adding in support for 4.2.17's... 6 years ago
 modules/events Switching to full PHP tags everywhere, adding in support for 4.2.17's... 6 years ago
 README.md README update 8 years ago
 manifest.json Added methods for getting a page of upcoming events, fixed SQL inj... 5 years ago

☰ README.md

About

An Events extension for BigTree CMS.

📖 Readme

☆ 1 star

👁 1 watching

🍴 3 forks

Releases

No releases published

Packages

No packages published

Then Why Does Grype Think This Is In Node?

Known Affected Software Configurations [Switch to CPE 2.2](#)

Configuration 1 ([hide](#))

 `cpe:2.3:a:events_project:events:*:*:*:*:*:bigtree_cms:*:*`

[Show Matching CPE\(s\)](#)▼

Up to (excluding)

2018-03-19

CPEs

cpe:2.3:a:events_project:events:*.~*~*~*~*:bigtree_cms:~*~*

Scheme Format [\[edit\]](#)

The CPE follows this format, maintained by NIST:^[2]

```
cpe:<cpe_version>:<part>:<vendor>:<product>:<version>:<update>:<edition>:<language>:<sw_edition>:<target_sw>:  
<target_hw>:<other>
```


So Now What?

```
{
  "@context": "https://openvex.dev/ns",
  "@id": "https://openvex.dev/docs/example/vex-9fb3463de1b57",
  "author": "Wolfi J Inkinson",
  "role": "Document Creator",
  "timestamp": "2023-01-08T18:02:03.647787998-06:00",
  "version": "1",
  "statements": [
    {
      "vulnerability": "CVE-2014-123456",
      "products": [
        "pkg:apk/distro/git@2.39.0-r1?arch=armv7",
        "pkg:apk/distro/git@2.39.0-r1?arch=x86_64"
      ],
      "status": "fixed"
    }
  ]
}
```

A VEX Statement

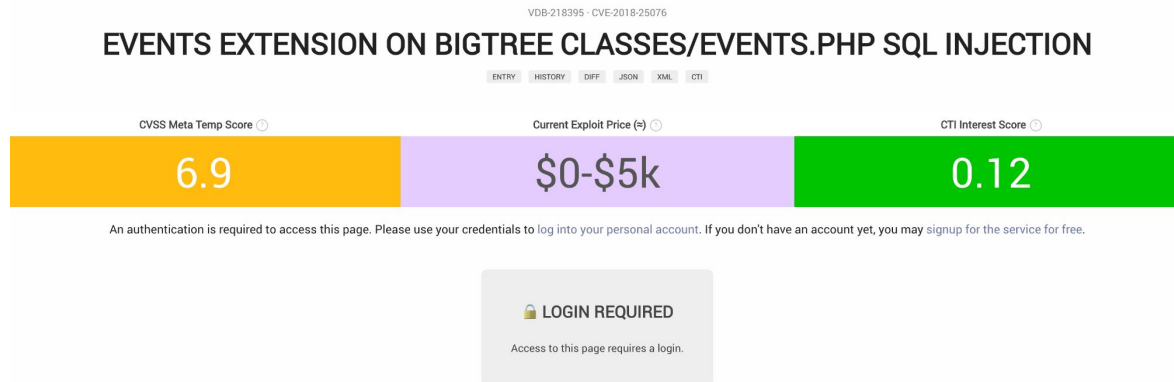
```
{
  "@context": "https://openvex.dev/ns",
  "@id": "https://openvex.dev/docs/example/vex-9fb3463de1b57",
  "author": "Wolfi J Inkinson",
  "role": "Document Creator",
  "timestamp": "2023-01-08T18:02:03.647787998-06:00",
  "version": "1",
  "statements": [
    {
      "vulnerability": "CVE-2018-25076",
      "products": [
        "pkg:oci/cgr.dev/chainguard/nodesha256:64060f28e2bbe5e970fa596de60f9652062659e9d8d823e5ce884d37395706ee"
      ],
      "status": "component_not_present",
      "impact_statement": "The vulnerable code is not present, it's a false positive match and the code is written in Node,"
    }
  ]
}
```

An Aside...

Why did a CVE just get reported a few weeks ago for a personal project that was last updated in 2018 with 1 star and it's not clear if anyone is using it?

An Aside...

Why did a CVE just get reported a few weeks ago for a personal project that was last updated in 2018 with 1 star and it's not clear if anyone is using it?



So that's Why VEX, Why OpenVEX?

- For this to work, we need scanners to implement VEX and trust our VEX statements - for our images
 - This requires a signing/attestation framework
- No scanners seem to support any VEX frameworks today
 - Our customers/users use snyk, gype, trivy, twistlock
- CSAF is large, unwieldy, and doesn't have working libraries in the languages we need
 - Philosophically, we prefer simple standards that do one thing well
- CDX supports VEX, but it not very usable for folks in the SPDX ecosystem
 - The documents can be generated standalone from an SBOM, but the toolchain is CDX centric
- **VEX as a whole is incredibly new, let's start fresh and get this right.**

Doesn't this fragment things?

- Meh, not really. There isn't much of anything to fragment
 - $0/3 == 0$
- There will be multiple formats no matter what, and users can pick which they prefer
- The CISA WG ****just**** published a definition for “what it means to be VEX”, and anything that implements that can be translated



@Pinboard

The Programmers' Credo: we do these things not because the but because we thought they were going to be easy

4:15 PM · Aug 5, 2016

8,037 Retweets 433 Quote Tweets 13.2K Likes



@msw@msstdn.social
@_msw_

I consider the "anti-fragmentation" movement that made it less socially acceptable to compete ("Join us under our Big Tent! No? You're doing your own open-source thing? You're not Open Sourcing Right by not joining us!") harmful.



Kelsey Hightower @kelseyhightower · 23h

One open source project implementing something doesn't disqualify another open source project from attempting to do the same.

This is a collaborative effort, not a game of Monopoly.

[Show this thread](#)

1:41 PM · Mar 3, 2023 · 20.3K Views

Also - Licensing/Patents

- We eventually intend to propose OpenVEX as an international standard (through ISO, IETF, or similar).
- OpenVEX is governed by the Community Specification process, which provides the necessary patent protections for specifications (above and beyond just normal CC and Apache/MIT licenses).
- International standard status and patent protections are a deal blocker for many organizations, and also a requirement for the OSSF.

OpenVEX Roadmap

- Make the spec!
- Work with OSS projects to produce VEX documents
 - Starting with our own or ones we help maintain
- Work with a few scanners to implement the spec and flesh out the trust model
 - Why should I trust this?
 - How do I configure what VEX sources I trust?
 - How do I see the individual entries and override them?
- Get more projects and scanners to support OpenVEX documents!
- Rinse and repeat!

VEX + SBOMS

Two technologies that work hand-in-hand to secure your software supply chains.

