nexB

Dennis Clark <dmclark@nexb.com>

When will there be VEX tools?

1 message

tom@tomalrich.com <hi@follow.it> Tue, Nov 7, 2023 at 8:23 AM
Reply-To: tom@tomalrich.com
To: dmclark@nexb.com

Tom Alrich's Blog

Edit

Unfollow

When will there be VEX tools?

by Tom Alrich Nov 7, 2023

Today, a very refreshing email was sent to the CISA VEX Workgroup mailing list:

> We're a small startup from Germany trying to establish a vulnerability management procedure for our own product and we wrote down our "dream setup" in a document: <https://docs.google.com/document/d/1QB3EaimrS0KIL6wIpfY5-SlEEYV_Y-hfM8_SGKjGNz0>
>
> ……
>
> Basically, we're struggling with the practical implementation bit of actually implementing a workflow to publish VEX statements. Everyone we talked to is building their own custom in-house solution (and we talked to a lot of companies by now).

I call this email “refreshing”, because, even though it didn’t point to any magic solutions, it at least pointed to the big problem with VEX: there are no standardized VEX production and consumption tools, because there is no standardized VEX specification. No vendor is going to produce a tool for VEX until they can build it to a specification (whether or not it’s an internationally recognized standard is irrelevant at the moment) that they’re sure will be followed by multiple VEX producers and consumers (it doesn’t have to gain universal acceptance, but at least be in use by multiple producer and consumer organizations).

The document (which I haven’t had time to go through in full yet) has already garnered a lot of good comments. I added one of my own, in reference to this entry in a list of problems with VEX: “Very little tooling around automatic generation and publishing of CSAF files exists.”

I commented:

It's that there's very little generation and publishing of CSAF files - at least, files that will be read as part of an automated process, as intended - but it's certain there's zero generation or publishing of CSAF *VEX* files. This is because there's never been a rigorous specification of what a CSAF VEX needs to contain (and specifically, there's never been a specification of the minimum that's required in the Product Tree and Branches fields, which are mandatory in any CSAF document and offer an absolutely huge number of options). This means that software producers are free to produce VEX files using any spec they want (I've counted at least four separate VEX specs in use, each addressing a completely different use case, and this doesn't cover the wealth of "private" VEX specs that must be in existence).

Until there is such a spec, there will never be production and consumption of VEX files in CSAF. While there are companies like Red Hat, Cisco and Oracle that publish CSAF VEX files now, none of them can point to any open source or commercial tool that ingests their VEX files and passes the results on to vulnerability management tools. And there never will be any such tool, until there is a rigorous VEX spec for CSAF (the same is needed for CycloneDX VEX, although the problem is much less severe in that case) that is followed both in production and consumption tools.

The OWASP SBOM Forum is now developing such a spec - first for CSAF VEX and then for CDX VEX. We may also develop prototype production and consumption tools, but in any case, tools should be easy to develop when this is done. If you would like to join this effort email tom@tomalrich.com

The author of the email, Lars Francke of Stackable, emailed me in minutes about joining this effort. The invitation is also open to *you*, Dear Reader!

Any opinions expressed in this blog post are strictly mine and are not necessarily shared by any of the clients of Tom Alrich LLC. If you would like to comment on what you have read here, I would love to hear from you. Please email me at tom@tomalrich.com.

I lead the OWASP SBOM Forum. If you would like to learn more about what that group does or contribute to our group, please go here.

Continue Reading

Follow more feeds