Breaking: What is Going on with the NVD? Does it Affect Me?

AJ Starita • March 14, 2024 • 5 min read

Application Security

Share article

Table of Contents

Headed by NIST, an American government institution, the National Vulnerability Database (NVD) contains vulnerability data that's been key to protecting organizations both within and without the US borders for more than 20 years. Many security policies from both commercial and government organizations require that vendors take care of vulnerabilities of a particular severity ***as given by the NVD*** within a certain number of days. It is not overstating things to say that it's the biggest and most important vulnerability database on earth.

And something has gone wrong with it.

On February 15th of this year, the NVD posted a notice to the top of its site stating,

"NIST is currently working to establish a consortium to address challenges in the NVD program and develop improved tools and methods. You will temporarily see delays in analysis efforts during this transition. We apologize for the inconvenience and ask for your patience as we work to improve the NVD program."

This didn't garner much attention at the time but as the weeks passed, analysts began to realize that the NVD was becoming ***seriously*** behind with fully reporting CVEs.

Before we get into what that means, let's take a quick step back and review how a CVE becomes an ***NVD*** CVE. Schoolhouse Rock wasn't available to make a song about it, but I'll try to keep it quick.

You down with NVD? (Yeah CVEs!)*

CVE stands for "Common Vulnerabilities and Exposures", which is a framework developed by MITRE, but most people use "CVE" as a singular noun and faster way to say "known security flaw that's already been assigned a CVE ID".

CVE IDs are reported by CVE Numbering Authorities, also known as CNAs, also known as about 350 large tech companies, security vendors (Mend.io is one), and researchers. Other people and organizations find vulnerabilities, too, but one way or another they find their way to CNAs who actually report them so they can become bonafide CVEs.

To recap the alphabet soup: A CNA reports a CVE; and it then gets a CVE ID and enters the NVD.

On its own, a CVE gives very little information. It gives a little bit of the ***what,*** but not the ***what kind***, ***where***, or the ***how bad***. Right away, when a CVE becomes public, the NVD adds it to the site, but it's not finished cooking yet. To be an official ***NVD*** CVE, it needs to be a fully tagged, meaning it needs to be mapped with a bunch of other cybersecurity acronyms, namely:

Common Weakness Enumerators (CWEs) – Another MITRE classic, CWEs describe the type of coding or architecture flaws that underlie a vulnerability. There are about 600 of them and they're not all strictly about security issues.

Common Vulnerability Scoring System (CVSS) – A CVSS score describes the impact severity of the CVE. We have written about this before, but it should be noted again that a base CVSS score is more of a worst-case scenario, not a declaration that everyone using software with a CVE is equally affected.

Common Platform Enumerator (CPE) – CPEs are just systems, software, and packages. It's kind of important to know what thing you have to be using to be in danger of a CVE. More on that in a minute.

If you didn't want a refresh, you can start reading again here

So now that we know that an NVD CVE is supposed to include CWE (what kind of problem), CPE (which thing in your stack), and CVSS (how bad it is), it becomes a little concerning to learn that for the past month, the NVD hasn't been tagging those things. In fact, since mid-February, ***thousands*** of CVEs have been left untagged.

The NVD has only tagged a measly 59 CVEs since February, leaving a full 40% of 2024 CVEs without vital information.

Not tagging CPE is a ***really*** big deal, as it's the main way to match a CVE to one of those components, and is relied on by many home-grown vulnerability solutions (but not Mend SCA!). So no CPE means those solutions won't know to match a vulnerability with a library -– it just won't show up.

What exactly is happening over at NIST/NVD to cause this huge backlog is anyone's guess. No one has made any statement, officially or otherwise.

Oh no! Am I affected?

Quite a few SCA solutions use the NVD as a sole or at least primary source of vulnerability information and if this is yours, then the lack of CPE data especially may be leading your SCA to fail to report CVEs that you are very much affected by. False positives are the usual SCA problem but here we've got a false negative problem. 2024 is shaping up to be a crazy year!

By the way, Mend SCA is ***not*** one of those SCAs. We source our information from many places, and we've ensured that we've covered what NVD is lacking. If you're a Mend SCA customer, you don't have to worry about this.

If you're using Mend Renovate and keeping your dependencies healthy and up to date, you're also all good. After all, updating to a later version is the recommended way to address most CVEs — so if you're up-to-date, you don't have to worry about the severity of a vulnerability you don't have.

*My deepest sympathy to anyone who did not get to enjoy the 1990s/musical stylings of Naughty by Nature.

About the author

AJ Starita

AJ Starita is fascinated by the challenges and triumphs of cybersecurity and open source software. When not writing about technology, AJ can usually be found exploring nature or reading detective novels.

Recent resources