Blog - Mend’s Handy Guide to Using EPSS Scores

Mend’s Handy Guide to Using EPSS Scores

AJ Starita • January 3, 2024 • 6 min read

Application Security

Share article

Table of Contents

EPSS is a relatively recent addition to the world of freely available security scoring systems. While it’s not without its flaws and limitations, EPSS can be a powerful predictor of exploits to come and a useful tool in your arsenal, as long as you wield it correctly.

What is EPSS and what does an EPSS score tell me?

The Exploit Prediction Scoring System (EPSS) is powered by volunteers from the public and private sector and is under the management of a security non-profit organization known as Forum of Incident Response and Security Teams (FIRST). EPSS is designed as a new approach to prioritizing vulnerability remediation. Designed for use as pre-threat intel, an EPSS score uses both CVE data and real-world exploit data to generate a percentage that represents “a daily estimate of the probability of exploitation activity being observed over the next 30 days”. The EPSS model makes use of over a thousand variables and machine learning to fine tune its predictive powers. While FIRST maintains a special interest group (SIG) for EPSS that is open to the public, the actual special sauce of producing an EPSS score is not publicly available.

EPSS and public exploits

Many common vulnerabilities and exposures (CVEs) are concerning but theoretical. When there's a real and known way of exploiting a CVE in the wild, you've got yourself a public exploit. Even a rather low severity CVE becomes a very high-priority threat when it has an exploit. Exploits range in maturity from proof-of-concept, such as an academic releasing a paper on how an exploit could be performed, all the way to high severity, where the exploits are already packaged as tools that are readily available to script kiddies.

An EPSS score predicts the likelihood of a vulnerability going from theoretical to having a public exploit in the near future, so you'd expect a vulnerability that already has an exploit to have an EPSS score of 100% but the EPSS model doesn't actually take into account if a public exploit already exists. The reasoning behind this is that just because a CVE has one known exploit, doesn't mean more can't be created.

What is the difference between CVSS and EPSS?

The Common Vulnerability Scoring System is a free and open standard for scoring the severity of a vulnerability based on multiple factors, one of which is its current state of exploitability, as in whether or not there is currently an exploit or exploits and the maturity of said exploit(s). FIRST is also the steward of CVSS, but the teams working on the scoring systems as well as the SIGs for each initiative are separate. CVSS scores do get updated, such as when new exploits are found, but they don't attempt to predict the future like EPSS scores do. A couple of other key differences:

Usage. CVSS calculators exist for you to determine the severity of any vulnerability, including those that are not yet publicly disclosed, whereas the models behind EPSS are closed source and thus EPSS scores are published only by FIRST and are presently only available for CVEs with IDs.

Complexity. Another difference is that the EPSS model is more complex and updated more frequently. Compared to EPSS, CVSS is a far more static and simple system, having just released its fourth version in its 18th year of existence, whereas EPSS is already on its third version and is only just coming up to its third birthday.

The creators of EPSS argue that the common security strategy of fixing vulnerabilities with a CVSS score of X or above (in their demonstration they use a threshold of 7 and above severity for CVSS and 10% and above for EPSS) results in a high amount of wasted effort as most of those vulnerabilities will not end up being exploited.

The benefit of prioritizing vulnerability remediation based on EPSS instead of CVSS is a reduced amount of effort and increased efficiency due to the large reduction of false positives. The cost is an increase in false negatives (in their demonstration, the number doubles). However, it should be noted that false negatives are very low to begin with, especially compared to the false positives of this strategy.

It is also worth noting that the documentation on EPSS compares its current version with CVSS 3.0. CVSS 4.0 has just been released and it does a better job of weighing temporal and environmental data (like exploitability and application context) in the final score, which means most CVEs will have lower scores under CVSS 4.0 than they did under CVSS 3.0.

The limitations of EPSS and some practical advice

EPSS scores can't be the be-all and end-all of prioritization metrics. As mentioned above, EPSS scores are only available for those CVEs that have IDs. Vulnerabilities that don't have IDs, like misconfigurations and zero days, are also important to look out for.

Your prioritization flow should begin with asking if there already is an exploit. If there is, then it should be prioritized, and the EPSS score isn't particularly relevant.

Confidence levels are not given separately but are baked into the EPSS score and the higher the EPSS score, the higher the confidence. This means that lower EPSS scores should be read along the lines of "we don't know" rather than "not an active threat". On the other hand, CVEs with high EPSS scores should be treated as if there is already a public exploit, because there's a very good chance there will be.

Those with very low risk tolerance and the budget to back it up should continue to rely on prioritizing via CVSS. Conversely, those with limited resources and more risk tolerance may benefit from prioritizing via EPSS. Those in the middle can leverage a strategy that uses both. Many software composition analysis (SCA) vendors provide proprietary prioritization scores that weigh CVSS and EPSS (and other elements). If you plan to do your own weighing, a comfortable threshold for either or both metrics will need to be established based on your organization's needs.

One extra bonus use of EPSS: even if your organization chooses not to rely on EPSS for prioritization, EPSS scores, unlike CVSS scores, can be combined and then utilized to measure and compare your security posture over time.

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