tenable | Research Report

The critical few: How to expose and close the threats that matter

There are probably not as many as you think–if you know your critical exposures

(we'll show you how)

Table of contents

"The secret of getting ahead is getting started."

– Various attributions, including Mark Twain

Introduction

For the moment, forget all those acronyms that have crept into our daily lives as security professionals. Sure, they can be useful. But let's just think about the facts and dig a bit deeper than the buzzwords.

The truth is, if you look across the thousands of vulnerabilities that keep you up at night, only 3% are true exposures that put your business at risk. And within that 3%, only a fraction of exposures really matter. But how do you know what's what?

In this report, we'll feature groundbreaking new research from Tenable that uncovers the truth about where enterprises are exposed and what they can do to close it.

3%

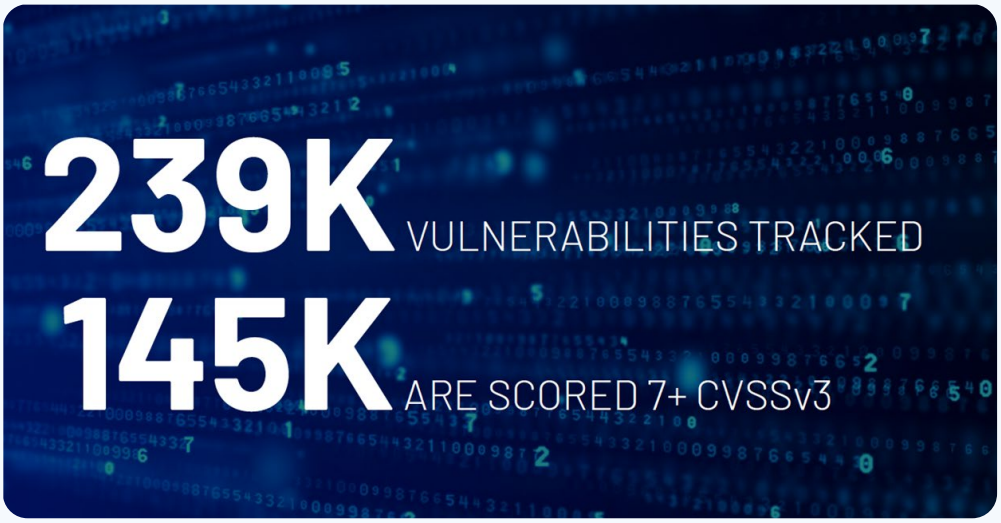
of all vulnerabilities are true exposures that represent a high likelihood of attack and material business impact.

Reducing Your Exposures

The first step in reducing your exposures is understanding which vulnerabilities are most likely to lead to harm. And that could be where it gets a little tricky. Vulnerabilities can be alternately informative and baffling. We think of them as big things. Their numbers mount. They're scary. Every day, there are more and more. They make for good headlines and they sure as heck keep a lot of folks up at night.

But, hang on. Is that really true?

Sure, there are 239,000 common vulnerabilities and exposures (CVEs) in the National Cybersecurity FFRDC (federally funded research and development center). One thing's for sure–that list of CVEs is a great resource.



The problem is that it can be a bit overwhelming.

239,000 CVEs? Are you kidding? I have to worry about a quarter of a million vulns? That's hard to fathom. Are they all the same kind of vulnerability? Do they all present the same threat level? And what about CVEs themselves–are they the only way to measure a threat? Good questions. Let's try to answer them.

Let's look at the range of ways to rank exposures. Sorry. We'll have to go a bit overboard on acronyms here.

OK, Get Ready for Some Acronyms

In addition to CVEs, there's the Exploit Prediction Scoring System (EPSS), described as "a data-driven effort for estimating the likelihood (probability) that a software vulnerability will be exploited in the wild." OK–that's helpful.

Then there's Common Vulnerability Scoring System (CVSS), which is essentially a score added onto the CVE.

That's a lot of acronyms and a lot of ways to measure the threat landscape.

How could anyone possibly focus on all of that?

We're here to tell you you don't. Stop worrying about the 239K and focus on the ones that matter–the critical few. Think of these vulnerabilities as dishes in your sink. You have a good dinner and you dirty some dishes. Wash those dishes as you use them every day and they're relatively easy to handle. Let them pile up for a few days and the task of cleaning up becomes daunting.

The Only Acronym You Need

Using our examination of most vulnerabilities, we calculate a Vulnerability Priority Rating. The VPR is a good companion to the data provided by the vulnerability's CVSS score.

And because we update the VPR to reflect the current threat landscape, it's a dynamic score. VPR values range from 0.1-10.0, with a higher value representing a higher likelihood of exploit. This table shows how those scores work.

VPR Category	VPR Range
Critial	9.0 to 10.0
High	7.0 to 8.9
Medium	4.0 to 6.9
Low	0.1 to 3.9

So, in plain English, a vuln with a VPR above 9.0 is likely to be exploited – and if you're exposed, these vulnerabilities would be the likely target. Looking further down the chart, vulns with a VPRs of 7.0 to 8.9 might be used by an attacker, but probably not. In addition, Mediums and Lows (from 0.1 to 6.9) are unlikely to be exploited.

Focus on the Critical Few

That's right, the important number isn't that top-line figure, although that's what might push you into action.

On the contrary, according to Tenable Research, the number you need to focus on is much lower.

Tenable is unique in looking at all of these vulnerabilities in minute detail so that we can identify the ones that require focus – and, remember, on an average day only about 3% of vulnerabilities are Critical or High.

Examining the Numbers from One Day

Let's look at some numbers from a recent day–June 2, 2024.

Our research shows that on that day, there were just under 240,000 vulnerabilities.

Using our VPR categorization, we found that only 3.1% of the vulnerabilities–or less than 7,500 – were at the Critical or High level. Drilling down even further reveals a more complete story.

Date	Critical	High	Low	Medium	% High & Critical
2024-06-02	853	6,627	94,170	138,272	3.1%

Of the nearly 240,000 vulnerabilities, 382 were ransomware vulnerabilities, 853 were at Tenable VPR 9 or above, 84 were persistently exploited, 1,124 were CISA known exploited, and 805 were known exploited vulnerabilities on the network attack vector.

Revealing the Life Story of a Vulnerability

Many of us might be familiar with the Myers-Briggs Type Indicator. It's a common tool that many organizations use to understand the personalities of employees and new recruits. One thing it does is classify people as extraverts or introverts. But that judgment requires context.

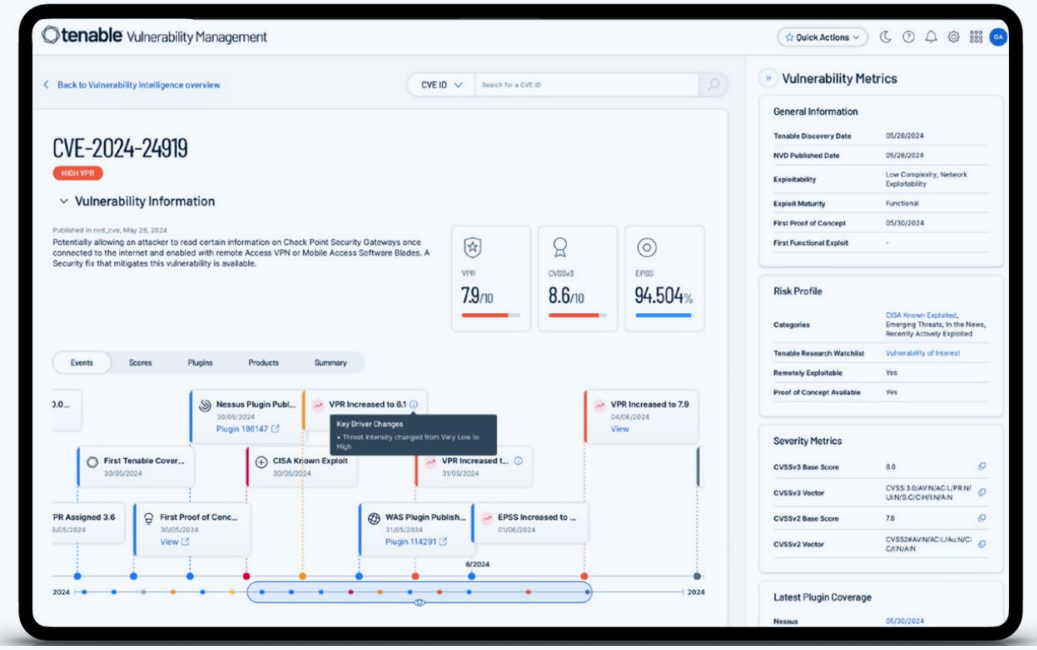
Some performers are introverts in their daily life but blossom into full-blown extraverts once on stage.

So the problem is, despite classifying someone in a rigid framework, Myers-Briggs doesn't really tell you much about the actual person in the context of their daily life. For an employer, the test might be worth using in certain circumstances when hiring a new team member but it certainly couldn't take the place of the standard employment background check.

And that brings us to CVSS – the Myers-Briggs of the cyber world. CVSS is a very superficial (and often inaccurate) measure of a vulnerability. Vulnerabilities are complex and not fixed in time, so a simple metric doesn't give you the full picture.

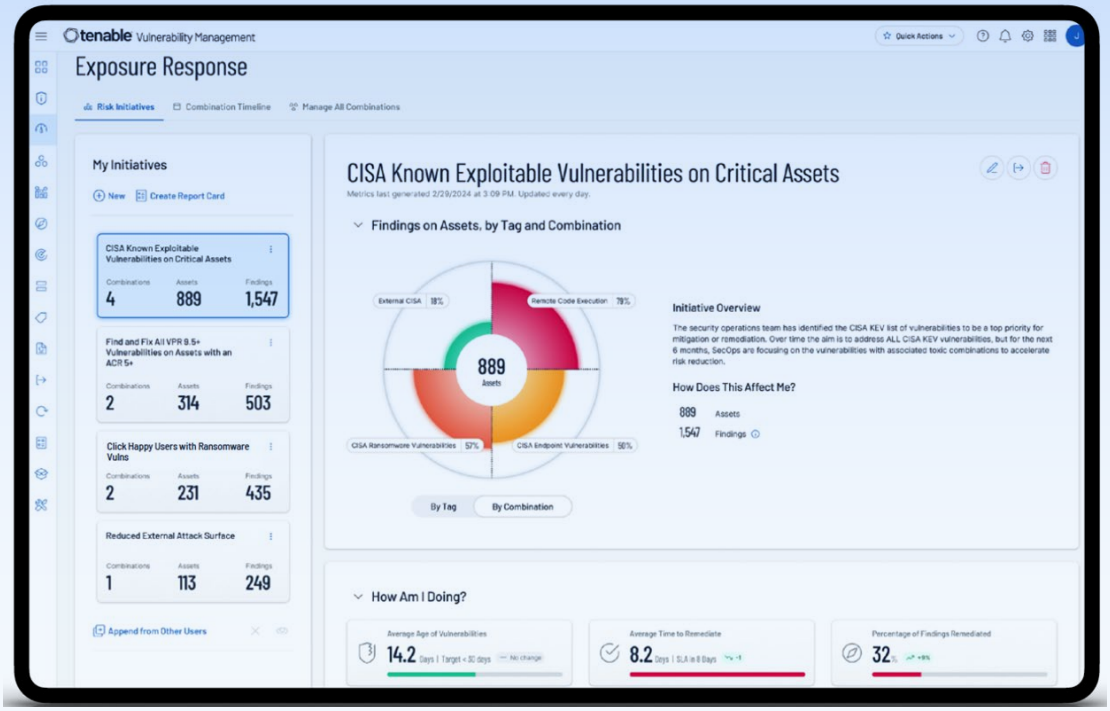
Enter VPR, which is like having a rich, detailed life story of a vulnerability.

The timeline in Tenable Vulnerability Management (see below) tells the story of a vulnerability – from birth to (hopefully) death. Like a background check on a person, you get a detailed view of the life of this vulnerability. Does it have a criminal record? Who has it been hanging around with?



Tenable Vulnerability Management points out the vulnerabilities that matter. In Exposure Response (see below), we provide a way to track how effectively you're addressing issues.

For example, although NIST dictates that a CVSS vulnerability of 7+ requires remediation within 90 days, that's not good enough. You need to fix that now. And we show you how.



VPR: The Secret to a Good Night's Sleep

If you're overwhelmed by the sheer number of vulnerabilities, take solace in the words we shared earlier – the secret to getting ahead is getting started. Maybe Mark Twain didn't have the advantage of VPR, but we think he'd admire the way it helps you move quickly.

With help from Tenable, you can take that seemingly impossible number and bring it down to something manageable. The 239,000 vulnerabilities suddenly become a handful of issues you can take care of methodically.

This approach will ensure your company is safer – and you might even sleep a bit more soundly.

In the interest of transparency, we have included the full severity distribution table on the **appendix data table**.

About Tenable

Tenable® is the exposure management company, exposing and closing the cybersecurity gaps that erode business value, reputation and trust. The company's AI-powered exposure management platform radically unifies security visibility, insight and action across the attack surface, equipping modern organizations to protect against attacks from IT infrastructure to cloud environments to critical infrastructure and everywhere in between. By protecting enterprises from security exposure, Tenable reduces business risk for more than 44,000 customers around the globe. Learn more at www.tenable.com.

Contact Us:

Please email us at sales@tenable.com or visit tenable.com/contact

072524