EACG
Enterprise Architecture Consulting Group

SECURITY DIALOGUES
No. 8 · 25 September 2026
Marcus Hale (PSIRT) · Tess Calder (red team) · Jessy Lang

The 9.8 That Was Never About You

Which number answers which question, and the homework behind them

A scanner flagged a 9.8. It cost Marcus a weekend, four engineers and four hours to show the code path was never reachable, while a 5.3 on an internet-facing service with no authentication and customer data stayed open. The 9.8 was correctly computed, just never about that deployment. Different numbers answer different questions.

BORROWED SEVERITY
A real number, about a system that is not yours.

1. Does it apply to us at all?

2. How much does it matter here?

3. Is it, or will it be, exploited?

THE NUMBERS, THE QUESTION EACH ANSWERS, AND WHAT TO DO

1	**CVSS Base Score** How bad is the vulnerability itself?	Computed once by the discloser from how it is reached, attack complexity, privileges, user interaction, scope and the confidentiality, integrity and availability impact. It is the same number for every installation on Earth and says nothing about whether it affects you. At best a sorting hint. It was also somebody's argument before you saw it: vendors and researchers lean on it in both directions.
2	**Temporal** How bad is it now?	The Base vector adjusted for where the vulnerability is in its life cycle: public exploit code, a weaponised toolkit, a vendor fix, confidence in the report. The same question as Base, kept current.
3	**Environmental Score** How much does it matter, given that it applies?	Adjust the Base vector for your reality: is the vulnerable configuration present, do your mitigations change the attack complexity, and rate the confidentiality, integrity and availability requirement of the asset (low, medium, high). Almost nobody fills it in, because it needs a decision about what each asset is worth.
4	**EPSS** How likely is exploitation in the next 30 days?	A separate model, not part of CVSS, trained on observed exploitation data. It outputs a percentage, not a severity, and can disagree sharply with CVSS: a 7.5 under one percent, a 5.4 above ninety percent.
5	**KEV** Has it been exploited in a real attack?	CISA's catalog of vulnerabilities with direct evidence of use in a real attack. Not a score and not a prediction: the maximum case, because it already happened, somewhere, to someone.
6	**VEX** Does it apply to this product at all?	A statement of affected, not affected, fix available or under investigation. A vendor can publish not affected when the vulnerable function is compiled out. That is no vulnerability for you, not a lower severity. Marcus's Saturday war room was a VEX question in disguise.
7	**Asset tier list** Decide what your systems are worth before the CVE arrives.	Three tiers, once, covering every system. Tag each system at onboarding, write the tier definitions in plain language a non-engineer can apply, and pre-compute the confidentiality, integrity and availability requirements per tier into the Environmental Score, so scoring a new CVE is a lookup, not a debate.

THREE POINTS TO KEEP

Look at reachability yourself
Tess walked into a network through a 5.3 on an exposed service and walked past a 9.8 three hops behind a boundary. The Base Score does not know your segmentation, network layout or authentication.

Context cuts both ways
A 5.4 on a dosage-calibration component became closer to a 9 once the availability requirement was rated honestly. The homework is not a tool for talking yourself out of patching.

Pay once, triage in minutes
The tier list took about six weeks, mostly to agree what critical means across teams. The next 9.8 took twenty minutes to triage instead of a weekend.

Listen to the episode
The 9.8 That Was Never About You and the rest of the series.
eacg.de
/en/podcast/s08-borrowed-severity

Digital Product Design
From the first idea to a viable first release.
eacg.de
/en/consulting/digital-products

PSIRT Services
Intake, assess and disclose vulnerabilities, built or run as a service.
eacg.de
/en/consulting/psirt

© 2026 EACG GmbH