Understanding vulnerability priorities: high, medium and low

Patchstack · https://www.aeserver.com/support/patchstack-vulnerability-priorities/

Every vulnerability found on your site is labelled **high**, **medium** or **low** priority. This is not the CVSS score you may have seen elsewhere. It is a practical rating of how urgently you need to act, and this guide explains what each level means and what to do about it.

Why not just use the CVSS score?

CVSS is the industry standard for scoring vulnerabilities, from 0.0 to 10.0. It measures how much damage a vulnerability could do if it were exploited. What it does not tell you is how likely that is. A vulnerability can score 7 or above and still be unlikely to affect your site, because exploiting it may require conditions that rarely occur in practice.

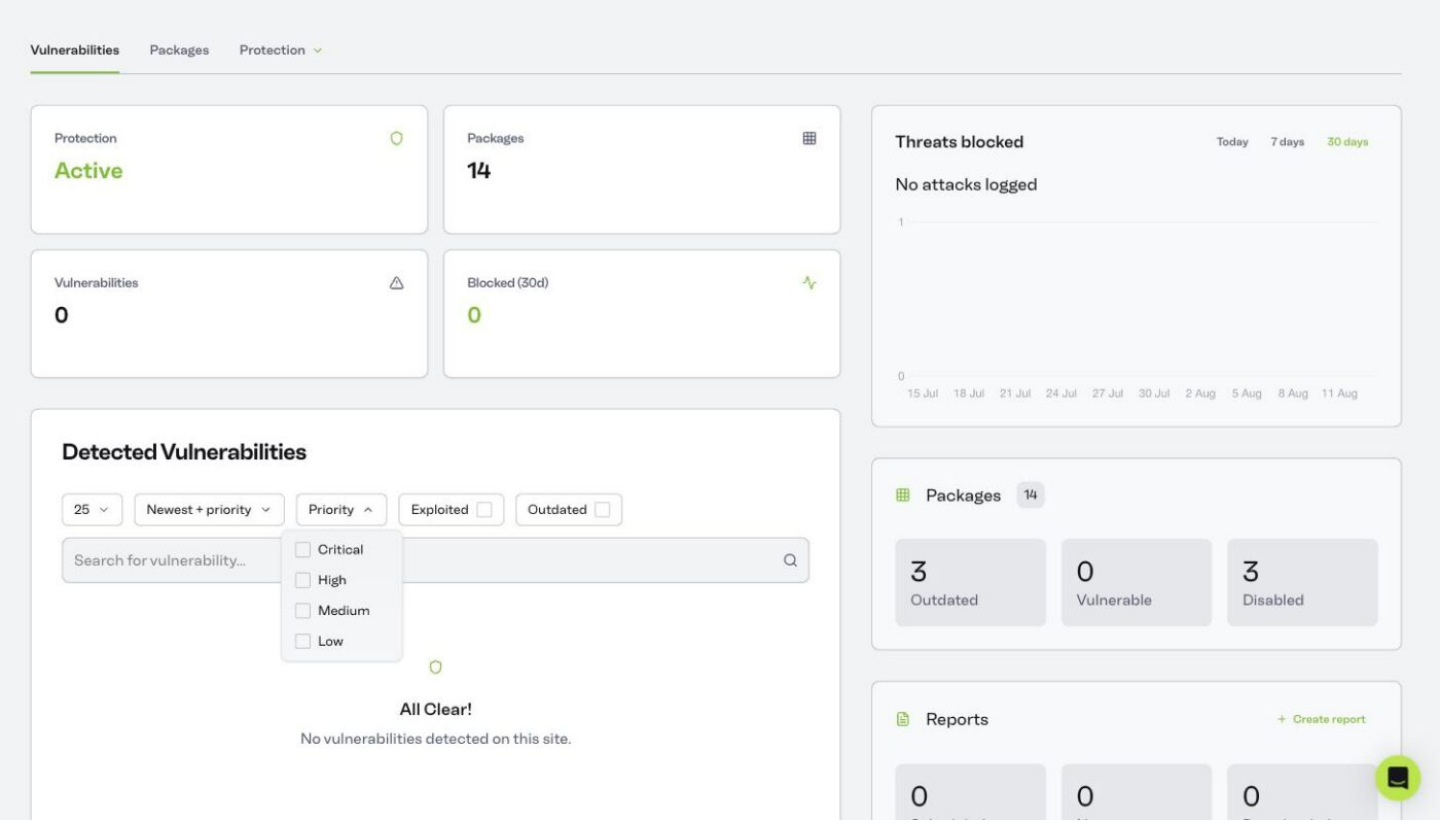
Relying on the score alone tends to produce long lists that all look urgent, which makes it hard to see what genuinely matters. Patchstack developed its own priority rating a few years ago for exactly this reason. It predicts how likely a vulnerability is to be exploited in the real world, taking into account factors such as the type of vulnerability, how widely the software is used and monitored exploitation attempts.

NoteThe priority you see is about **real-world risk**, not theoretical severity. A "low" priority item is not a mistake or an oversight; it means it is unlikely to be exploited.

The three priority levels

Priority	Act within	What it means	Mitigation rule
High	Immediately	Already being actively exploited in the wild, or expected to be very soon. Treat this on a zero-day timeline.	Applied automatically

Priority	Act within	What it means	Mitigation rule
Medium	7 days	Could realistically be weaponized in a targeted attack, but there is no evidence yet of active exploitation.	Applied automatically
Low	30 days	Not expected to be exploited, with no signs of real-world attacks. Handle on your normal maintenance schedule.	Not applied



The priority filter in your vulnerability list.

NoteYou may also see a **Critical** option in the priority filter. Treat anything marked Critical the same way as High priority: act on it immediately. In the full Patchstack portal, the levels may be labelled **Highly exploitable** (high), **Exploitable** (medium) and **No to low impact** (low).

High priority: patch immediately

These vulnerabilities are either being actively exploited right now or are expected to be within a very short window. Attackers are scanning for them, and an unprotected site running the affected software is a realistic target.

In almost all cases a mitigation rule is deployed automatically, so your site is shielded from the moment the vulnerability is known. Your job is still to apply the official update as soon as you reasonably can, because the mitigation rule buys you safe time rather than replacing the fix permanently.

Medium priority: patch within 7 days

These could be used against you in a deliberate, targeted attack, but nobody is currently exploiting them at scale. They also receive a mitigation rule automatically, so you are covered while you schedule the update.

A week is a sensible window: soon enough that you are not carrying avoidable risk, relaxed enough that you can test the update properly before it goes live.

Low priority: patch within 30 days

These are not expected to be exploited and show no signs of real-world attacks. They do not receive mitigation rules, because doing so would add rules to your site for no practical benefit.

Roll these into your normal maintenance cycle. If you already update plugins and themes monthly, a low priority item usually resolves itself as part of that routine.

TipIf you manage many sites, work top down: clear every high priority item across the whole portfolio first, then mediums, then lows. That ordering removes the most real risk for the least effort.

Why an alert is not bad news

ImportantSeeing vulnerabilities listed does **not** mean your site has been hacked or that protection has failed. It means the software on your site was checked against the vulnerability database and matches were found. In most cases they are already mitigated, and the list is simply telling you what to update and when.

A site with zero listed vulnerabilities is not necessarily safer than one with several; it just happens to be running software with nothing currently known against it. What matters is that anything found is mitigated quickly and updated in good time.

Get Patchstack Protection Prioritized alerts mean you always know what actually needs attention.

See pricing and get started.