The first 24 hours after a new CVE

A checklist for founders and CTOs

When a new security flaw (a CVE) is published, you do not need to become a researcher overnight. Work through the same three checks we use in our business triage notes, and keep a written record as you go.

CVE OR ISSUE NAME	DATE YOU HEARD ABOUT IT	OWNER

Check these three things.

- [ ] 1 **System owner: do you run an affected version?**
  Ask whether you use the affected product, service, or library, including software a vendor runs for you. Then check whether your version is one the vendor lists as affected.

- [ ] 2 **Network owner: is it exposed to the internet?**
  Check whether the system can be reached from the internet. Internal-only systems still matter, but internet-facing ones usually come first.

- [ ] 3 **Security owner: is it already being used in attacks?**
  Check whether the vendor or researchers say it is being exploited. Also check the U.S. government's catalog of known exploited vulnerabilities (CISA KEV). If it is not on that list, exploitation is unknown, not safe.

Why it matters

Urgency depends on whether you run an affected version, whether it can be reached from the internet, and whether it is already being used in attacks.

A listing in CISA's Known Exploited Vulnerabilities catalog, or a vendor report of exploitation, raises priority. This does not show harm at your organization. Only your records can show what happened.

Do Now

System owner: apply the vendor patch or official workaround.
If you cannot patch yet, restrict who can reach the system. This lowers exposure. It is not the fix.

Name who will confirm the facts, and who can approve a change.
If a vendor runs the system, write down who you will contact.

Do Next

Record what you checked, what you decided, and what is still unknown.

Tell customers or partners if they need to know.
Share only what you can confirm. Keep sensitive detail redacted unless the recipient needs it.

Agree when you will look again for a vendor update or new evidence of exploitation.

FOR YOUR IT TEAM

Founders and CTOs can skip this box. These are the technical checks that support the steps above.

- Record the exact product name and version, for example from a version command or the vendor's version page. Compare it with the versions the vendor lists as affected.
- Confirm whether the service is reachable from the public internet, and note the hostname and port.
- Read the vendor advisory, then check the `CISA Known Exploited Vulnerabilities catalog`. If a patch or official workaround exists, plan and apply it. Keep versions, timestamps, and sign-off with this checklist.

For a short, evidence-based starting point on many newly published issues, see **integritylab.ai/cvehit**. It is not a finding about your systems.

This checklist is general guidance. It is not an assessment of your systems and is not a substitute for advice about your environment. If you need a human-reviewed assessment package, start at integritylab.ai.