CHECKLIST

Vulnerability Prioritization Checklist: CVSS + Exploit Data

A practical checklist for ranking vulnerabilities by combining CVSS, exploit evidence, asset exposure, compensating controls, and business criticality.

Vulnerability Prioritization Checklist: CVSS + Exploit Data

Use this checklist to turn vulnerability scan results into a defensible remediation queue. It is designed to help teams avoid over-prioritizing high-scoring but low-reach findings and under-prioritizing vulnerabilities that are actively being exploited.

How to use this checklist

- Start with the CVSS base score and vector.
- Add exploit evidence and asset exposure.
- Verify compensating controls and business criticality.
- Assign a priority tier based on the combined picture.
- Document the reason for any override.

---

1) Confirm the vulnerability details

- [ ] Verify the vulnerability identifier, affected product, version, and asset.

- [ ] Record the CVSS base score.
- [ ] Capture the full CVSS vector.
- [ ] Note whether the finding is local, adjacent, internal, or internet-facing.
- [ ] Confirm whether the finding is present in production, staging, or lab systems.

Record:

- Vulnerability ID: _____
- Asset / hostname: _____
- Environment: _____
- CVSS score: _____
- CVSS vector: _____

---

2) Assess exposure

- [ ] Is the asset reachable from the internet?
- [ ] Is it reachable from partner networks or third parties?
- [ ] Is it accessible only internally?
- [ ] Is it segmented behind firewall, ACL, or bastion controls?
- [ ] Is the affected component disabled, isolated, or not deployed?
- [ ] Does the service accept untrusted input from users, clients, or external systems?

Exposure notes:

- _____
- _____

---

3) Check exploit evidence

Look for signs that the vulnerability matters now, not just in theory.

- [ ] Public proof-of-concept code exists.
- [ ] Reliable weaponized exploit code exists.
- [ ] The issue is included in exploit kits or commodity tooling.
- [ ] Threat intelligence reports active exploitation.
- [ ] Vendor or trusted research sources confirm abuse in the wild.
- [ ] Internal telemetry shows scanning, exploitation attempts, or suspicious traffic.
- [ ] The exploit appears practical in your environment, not just in a lab.

Exploit maturity:

- [ ] None known
- [ ] Proof of concept only
- [ ] Weaponized or reliable exploit
- [ ] Active exploitation observed

Evidence source(s):

- _____
- _____

---

4) Evaluate business and operational criticality

- [ ] Does the asset support identity, authentication, or privileged access?
- [ ] Does it support core production workloads?
- [ ] Does it store sensitive or regulated data?
- [ ] Would compromise enable lateral movement or privilege escalation?
- [ ] Would exploitation create outage, data loss, or customer impact?
- [ ] Is the asset part of a management plane, remote administration path, or backup system?

Criticality notes:

- _____
- _____

---

5) Review compensating controls

- [ ] Network segmentation limits who can reach the asset.
- [ ] Strong authentication is required.
- [ ] MFA is enforced for administrative access.
- [ ] A WAF, reverse proxy, IPS, or filtering control is in place.
- [ ] EDR, monitoring, or detection coverage is active.
- [ ] Hardening or configuration changes reduce attack surface.
- [ ] The exploit path is blocked by existing controls.
- [ ] Control effectiveness has been validated recently.

Control gaps or weaknesses:

- _____
- _____

---

6) Apply a prioritization decision

Use CVSS as the baseline, then adjust based on exploit evidence and exposure.

Escalate to highest priority if any of the following are true:

- [ ] The asset is internet-facing and exploitation is credible.
- [ ] Active exploitation is confirmed or strongly suspected.
- [ ] The vulnerability affects identity, remote administration, or sensitive data paths.
- [ ] The attack path is simple and the control environment is weak.

- [ ] The issue is being targeted in your environment.

Raise priority if:

- [ ] Public exploit code exists.
- [ ] The affected system is exposed to untrusted networks.
- [ ] The asset is business-critical.
- [ ] The vulnerability could enable lateral movement or privilege escalation.

Defer cautiously if all are true:

- [ ] The system is not exposed to untrusted networks.
- [ ] Strong compensating controls are in place.
- [ ] Exploitation requires difficult preconditions.
- [ ] No exploit evidence or targeted interest is present.
- [ ] A tracked remediation plan still exists.

Assigned priority tier:

- [ ] Emergency
- [ ] Urgent
- [ ] Standard
- [ ] Backlog

Decision rationale:

- _____
- _____

---

7) Validate before operational use

Before you rely on the ranking in production operations, confirm:

- [ ] The affected asset list is current.
- [ ] Exposure data reflects the real network path.
- [ ] Compensating controls are working as expected.
- [ ] The exploit evidence is credible and up to date.
- [ ] Ownership for remediation is clear.
- [ ] Maintenance windows and rollback options are known.
- [ ] Dependencies and service impact are understood.
- [ ] The ranking was reviewed by security and system owners if needed.

---

8) Document exceptions and overrides

If you override a CVSS-based rank, write down why.

Include:

- [ ] What signal changed the priority
- [ ] What evidence supported the decision
- [ ] What control or exposure factor mattered most
- [ ] Who approved the exception
- [ ] When the item will be rechecked

Override record:

- Vulnerability: _____
- Original rank: _____
- New rank: _____
- Reason for change: _____
- Approved by: _____
- Review date: _____

---

9) Suggested operating rule set

Use these simple rules to keep prioritization consistent:

- Treat CVSS as the starting point, not the final answer.
- Promote externally reachable vulnerabilities with credible exploit evidence.
- Prioritize identity, administrative, and data-exposure paths.
- Downgrade only when exposure is limited and compensating controls are strong.
- Document every override so the process remains defensible.

Quick review summary

A vulnerability should move up the queue when it combines:

- high or moderate severity,
- real exposure,
- credible exploit evidence,
- weak or unverified controls,
- and meaningful business impact.

A vulnerability may move down when it is:

- isolated,
- well controlled,
- difficult to exploit,
- and not associated with active abuse.

One-line decision template

Prioritize this finding because:

[CVSS severity] + [exposure level] + [exploit evidence] + [business impact] + [control effectiveness] = [priority tier]

Reminder

The goal is not a perfect score. The goal is a repeatable, evidence-driven queue that helps the right people fix the right vulnerabilities first.