

GHOST DEFENSE

Grounded Handling Of Sourced Threat-intel

VULNERABILITY EXPLOIT PRIORITY RANKER V E P R

OPERATIONS MANUAL

Standard Operating Procedure for Vulnerability Triage

Tool 06 · Build 2026.10.16-B · 16 October 2026

This manual governs how VEPR is run as a program: who holds which decision,
on what cadence, and what evidence is retained.

For operating instructions, see the VEPR How-To Guide.

TEMPLATE — adapt roles, cadence and thresholds to your organization

For defensive and authorized security use only · DEFEND ALWAYS.

Not a CISA product. Carries no CISA endorsement.

1. PURPOSE AND SCOPE

1.1 Purpose

This manual establishes the standard operating procedure for using VEPR to triage vulnerabilities, assign remediation timelines, and produce defensible evidence of those decisions. It defines who holds each decision, the cadence on which triage runs, and what is retained for audit.

1.2 Scope

- **In scope:** Vulnerabilities identified by the organization's own scanning programme, imported into VEPR as scanner output or as a CVE list.
- **Out of scope:** Asset discovery, vulnerability scanning, patch deployment, and configuration management. VEPR consumes scan results; it does not produce them.

1.3 Relationship to the How-To Guide

The How-To Guide explains how to operate the tool. This manual explains how the organization operates the process. Where the two differ on a procedural point, this manual governs.

1.4 Authorities and references

Reference	Applied to
CISA BOD 26-04 — Prioritizing Security Updates Based on Risk	Remediation deadline assignment
CISA SSVC Guide (November 2022), Tables 8 and 9	SSVC outcome determination
CISA Known Exploited Vulnerabilities catalog	Confirmed in-the-wild exploitation
Organizational vulnerability management policy	Exception handling, risk acceptance

2. ROLES AND DECISION AUTHORITY

VEPR derives what public data can support and withholds the rest. Every withheld value corresponds to a decision a named person must make. This section assigns them.

2.1 Roles

Role	Responsibility in this process
VM Operations Coordinator	Runs the triage cycle, operates the tool, consolidates inputs, issues tasking, retains evidence. Owns this SOP.
System Owner	Sole authority to assert Technical Impact for systems they own. Accountable for remediation within the assigned timeline.
Network / Infrastructure	Authoritative source for Publicly Exposed. Confirms whether an affected asset is reachable from the public internet.
Scanning / Assessment	Supplies the scan exports that feed VEPR. Accountable for coverage and currency of the scan data.
CISO / Authorizing Official	Approves exceptions, deviations from assigned timelines, and formal risk acceptance.

2.2 Decision authority matrix

No person may assert a variable outside their column. A value asserted by the wrong role is an audit finding even when the value is correct.

Variable	Authority	May not be set by	Basis required
In KEV	Automatic — CISA KEV catalog	Anyone (not overridable)	None; source of record
Publicly Exposed	Network / Infrastructure	VM Coordinator acting alone	Current network or ASM evidence
Automatable	VM Coordinator, or CISA Vulnrichment	System Owner	Named exploit tooling or CISA value
Technical Impact	System Owner	VM Coordinator, CISO	Configuration knowledge of the deployment
Mission & Well-being	CISO / mission owner	VM Coordinator acting alone	Documented mission dependency

THE TECHNICAL IMPACT RULE A System Owner asserting Technical Impact is answering one question: does this flaw give an attacker FULL CONTROL of the vulnerable component as it is actually deployed here? TOTAL means yes. PARTIAL means anything less. It is NOT a statement about how important the system is. BOD 26-04 contains no mission variable, deliberately, so the same flaw carries the same deadline across every agency. An owner who answers TOTAL because the system is critical has inflated the tier and the output is no longer the directive. Mission weight is captured separately, in SSVC Mission & Well-being, by the CISO.

3. OPERATING CADENCE

Cycle	Trigger	Actions	Owner
Daily	Start of business	Refresh KEV and exploit intel. Review any new P1. Confirm no 3-day BOD item is approaching breach.	VM Coordinator
Weekly	Scheduled	Full triage cycle against the current scan export (section 4). Issue tasking. Publish the report.	VM Coordinator
Monthly	Scheduled	Review exceptions and overdue items. Re-validate exposure settings. Audit a sample of operator-asserted values (section 7).	VM Coordinator + CISO
On trigger	New KEV entry affecting a known asset; emergency directive; active incident	Immediate out-of-cycle run limited to the affected products.	VM Coordinator

THE 3-DAY TIER DRIVES THE DAILY CYCLE The shortest BOD 26-04 timeline is three days, and the 3-day-with-triage tier additionally requires forensic assessment before patching. A weekly-only cadence cannot reliably meet a three-day clock. The daily check exists specifically to catch those items on day one.

4. STANDARD TRIAGE PROCEDURE

The weekly cycle. Phases run in order; later phases depend on earlier ones being complete.

Phase 1 — Intake

1.1 Obtain the current scan export

Pull the latest Nessus .nessus, Qualys CSV or nmap XML from the scanning team. Record the scan date. A scan older than the organization's scan-currency standard is rejected and returned, not triaged — stale input produces confident wrong answers downstream.

1.2 Import into VEPR

Use IMPORT SCAN rather than pasting a CVE list. The import carries host, port and service, so every finding downstream knows which assets it sits on. Confirm the imported host count matches the scan.

Phase 2 — Enrichment

2.1 Load the live KEV catalog

Confirm it loaded. If the catalog is empty VEPR withholds ranking rather than reporting a false all-clear; if you see that state, the fetch failed and must be resolved before proceeding.

2.2 Load exploit intelligence

Required. Without it every KEV item is capped at P3 and the exploit column reads NOT CHECKED. Confirm at least two of the three feeds report OK. Record which feeds succeeded.

2.3 Load CISA Vulnrichment

Supplies CISA-published Automatable and Technical Impact. Roughly half of CVE records are unenriched; those will require operator input in Phase 3.

Phase 3 — Operator input

3.1 Set Publicly Exposed

Obtain from Network / Infrastructure. Set the estate default where one applies, then override per-CVE for exceptions. Until exposure is set, timelines display as a span at the worse case.

3.2 Set Mission & Well-being

Obtain from the CISO or mission owner. Until set, SSVc outcomes display as ranges and rows sort by worst case.

3.3 Collect Technical Impact assertions

For findings where Vulnrichment supplied no value, route to the System Owner of record. Do not assert on their behalf. An unanswered item stays unanswered — VEPR will withhold the tier and name the missing variable, which is the correct and auditable outcome.

Phase 4 — Adjudication

4.1 Work the P1 list first

P1 means in KEV and a weaponized public exploit exists. Treat as immediate tasking.

4.2 Reconcile disagreement between the three verdicts

Priority, SSVC and BOD can disagree. Where they do, identify which input differs and record the reasoning. A P1 landing at 14 days under BOD usually means the asset is not exposed; an SSVC ACT with no BOD tier usually means Technical Impact is unknown.

4.3 Flag forensic-triage items

Any finding in the 3-day-with-triage tier requires compromise assessment BEFORE patching. Route these to incident response in parallel with the patch tasking. Patching does not evict an attacker who is already resident.

Phase 5 — Tasking and evidence

5.1 Issue tasking

Each item carries the CVE, the affected assets, the assigned timeline, and the deadline date.

5.2 Export and retain

Produce the printable report, the findings CSV and the JSON run manifest. Retain per section 6.

5. DATA SOURCES AND DEGRADED-MODE OPERATIONS

5.1 Freshness requirements

Source	Requirement	If breached
CISA KEV	Refreshed within 24 hours of the run	Re-fetch. Do not triage on an empty catalog.
Exploit intel	Within 24 hours	VEPR marks it stale and withholds SSVC outcomes. Refresh.
Scan data	Per organizational scan-currency standard	Reject and request a current scan.
Vulnrichment	Per run, on demand	Proceed; collect Technical Impact from System Owners instead.

5.2 Degraded modes

Condition	Operating posture
Exploit intel unavailable	Triage continues on KEV certainty alone. All KEV items cap at P3 and the exploit column reads NOT CHECKED. Record the degraded run in the manifest. Do not report P3 as "no exploit exists" — it means the check did not run.
Exploit-DB feed failing, others healthy	Acceptable. Exploit-DB is the only feed requiring a proxy hop. Metasploit and Nuclei results remain valid. Note the gap in the run record.
No external network (air-gapped)	Load the KEV catalog from file via UPLOAD KEV FILE. Ranking works; the exploit-availability layer does not. Treat every output as exploit-status-unknown.
Vulnrichment unavailable	Technical Impact falls to the CVSS vector, labelled as such, or to System Owner assertion. Prefer the owner assertion.
Tool itself unavailable	Fall back to KEV due dates and organizational policy. Record the gap; re-triage the backlog when restored.

6. EVIDENCE AND RECORDKEEPING

The defensibility of a triage decision rests on being able to show, later, what was known at the time and who asserted what. Retain the following for each cycle.

Artifact	Contains	Retain
Printable report (PDF)	Ranked findings, methodology and provenance block, guide edition, which factors were derived vs asserted	Per records schedule
Findings CSV	Per-CVE rows with assigned tier and affected assets	Per records schedule
JSON run manifest	Run provenance — sources used, feed status, freshness timestamps	Per records schedule
Operator input record	Who asserted exposure, Technical Impact and Mission & Well-being, and when	Per records schedule
Source scan export	The input the run was built from	Per records schedule

THE PROVENANCE BLOCK IS THE AUDIT ARTIFACT The printed report states which factors were derived from public data, which were analyst-set, and which were operator-supplied, and marks analyst-set values "(analyst)". That separation is what allows a reviewer to distinguish a tier resting on published fact from one resting on judgement. Do not strip or summarise it when forwarding the report.

6.1 Settings persistence — a caution

Exposure settings, Mission & Well-being and operator overrides persist in browser local storage on the individual workstation, under ghost06_* keys. They are not shared, not backed up, and are lost if site data is cleared. Treat the exported manifest as the record of what was asserted — not the browser.

7. QUALITY CONTROL

Before tasking is issued, the VM Coordinator confirms the following. Any "no" stops the cycle.

- The KEV catalog loaded and is current; no run was performed against an empty catalog.
- At least two exploit-intel feeds reported OK, and intel is under 24 hours old.
- The imported host count matches the source scan.
- No finding carries a tier derived from a variable asserted by a role without authority for it.
- Every 3-day-with-triage item has been routed to incident response as well as to patching.
- Items with withheld tiers are listed as withheld in the tasking, not silently dropped.
- The report, CSV and manifest have been exported and retained.

7.1 Monthly assurance sample

Each month, sample at least five operator-asserted Technical Impact values and confirm with the System Owner that the assertion reflects component control rather than system importance. Systematic inflation of this variable is the most likely way this process degrades, because it is the one input with no external check on it.

8. METRICS

Metric	Why it is tracked
P1 findings open, and age of oldest	Direct measure of exposure to weaponized exploits
Items within each BOD tier, and count past deadline	Directive compliance posture
Findings with a withheld tier	Measures missing operator input, not risk — a backlog of unanswered questions
Percentage of findings with exposure set	Data-completeness measure; low values mean timelines are being read at worst case
Mean time to remediate, by tier	Whether assigned timelines are actually being met
Degraded runs per month	Health of the data-source chain

DO NOT REPORT WITHHELD TIERS AS COMPLIANT OR NON-COMPLIANT A withheld tier means a question has not been answered, not that a deadline has been met or missed. Reporting it in either column converts missing information into a false finding. Track it as its own number.

APPENDIX A — WEEKLY RUNBOOK CARD

One-page summary for the operator. Full procedure in section 4.

#	Action	Confirm before moving on
1	Import current scan export	Host count matches the scan
2	LOAD LIVE KEV	Catalog is populated and current
3	LOAD EXPLOIT INTEL	At least two feeds OK; under 24h old
4	LOAD CISA VULNRICHMENT	Loaded; unenriched CVEs identified
5	Set Publicly Exposed (from Network)	Estate default set; exceptions overridden
6	Set Mission & Well-being (from CISO)	Both fields set; SSVC no longer ranging
7	Route unknown Technical Impact to System Owners	Requests sent; no self-assertion
8	Work the P1 list	Each P1 has an owner and a date
9	Flag 3-day-with-triage items to IR	IR acknowledged, in parallel with patching
10	Export report, CSV, manifest; retain	All three stored per records schedule

APPENDIX B — EXCEPTION HANDLING

An exception is a documented decision not to remediate within the assigned timeline. It is not a quiet omission from the tasking list.

Element	Requirement
Raised by	System Owner, in writing
Approved by	CISO or Authorizing Official — not the VM Coordinator
Must state	The CVE, affected assets, assigned tier, the reason remediation cannot meet the timeline, and the compensating controls in place
Expiry	Fixed date. An exception without an expiry is a risk acceptance and must be processed as one.
Review	Monthly, in the cycle described in section 3
Recorded in	The run record, so the report and the reality do not diverge

APPENDIX C — KNOWN LIMITATIONS REGISTER

Carried in this manual so that operators are not surprised by them mid-cycle, and so that nobody reads a gap as a finding. Review at each tool update.

Limitation	Operational consequence	Status
P2 cannot currently be assigned — the public proof-of-concept feed is declared but not populated	KEV items with a PoC but no weaponized module appear as P3. Read P3 as "KEV, exploit status not fully characterised".	Open
BOD 26-04 decision table transcribed from two secondary sources that agree, not yet diffed against the directive text	Verify against the directive before a tier drives a reportable deadline.	Open — verification required
Exploit-DB feed depends on a proxy hop	That feed may silently not load while the other two succeed. Check feed status each run.	Accepted
Absence of a public exploit is absence of evidence	Private and nation-state tooling is not observable. NONE FOUND is not proof of safety.	Inherent
Technical Impact falls back to the CVSS vector as a proxy	CISA does not define the variable via CVSS. Prefer System Owner assertion.	Mitigated by owner override
Settings persist only in the local browser	Not shared or backed up. The exported manifest is the record.	Accepted

GHOST DEFENSE

Grounded Handling Of Sourced Threat-intel

Zero-install, browser-based defensive security tooling
for resource-constrained organizations.

[ghost2210 . pages . dev](https://ghost2210.pages.dev)

DEFEND ALWAYS.