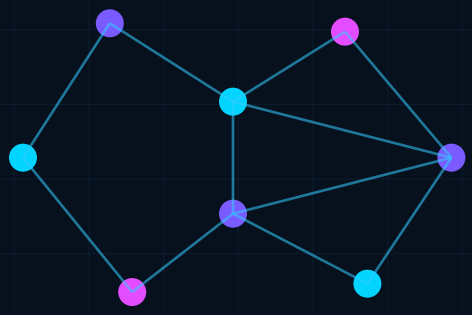
VULNERABILITY AND EXPOSURE MANAGEMENT

CISA KEV + EPSS + CVSS (Exploitability Prioritization Models)

Current-source review, evidence-bounded adoption decision, explicit limitations, reproducibility controls, and preserved source research note.



PERMANENT ID	EVIDENCE	ADOPTION	FRESHNESS
RES-004	A	ADOPT NOW	ACTIVE WATCH

Freshness review: 2026-09-17 / Next scheduled review: 2026-12-16

RESEARCH CONTROL SURFACE

Required Research Fields

Each field remains independently reviewable; evidence strength does not imply production authority.

EVIDENCE GRADE — **A**

Strength of the retained source set and technical basis.

SOURCE AUTHORITY — **3 registered authorities**

CISA Known Exploited Vulnerabilities Catalog; FIRST EPSS User Guide; FIRST CVSS v4.0 Specification and Guidance

FRESHNESS — **ACTIVE WATCH**

Reviewed 2026-09-17; dynamic sources require event-driven revalidation.

CONFLICTS — **VISIBLE / NOT SILENT**

Differences between specification, vendor behavior, research claims, and reproduced evidence must remain explicit.

LIMITATIONS — **EXPLICIT**

No certification, procurement approval, legal conclusion, or unbounded production claim is created by this report.

REPRODUCIBILITY — **REQUIRED**

Material claims require exact versions, representative data, failure cases, artifacts, and repeatable acceptance criteria.

ADOPTION POSTURE — **ADOPT NOW**

Adopt a composite prioritization model that combines active exploitation, exploit probability, technical severity, asset exposure, business criticality, compensating controls, and remediation feasibility.

REVIEW TRIGGER — **2026-12-16**

Scheduled at 90 days; earlier on material source, vulnerability, implementation, or contradictory-evidence change.

SOURCE AUTHORITY / FRESHNESS

Authority Register and Freshness Delta

Primary-source lineage is preserved; current-source changes are separated from unperformed implementation claims.

AUTHORITY 01

CISA Known Exploited Vulnerabilities Catalog

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

AUTHORITY 02

FIRST EPSS User Guide

https://www.first.org/epss/user-guide

AUTHORITY 03

FIRST CVSS v4.0 Specification and Guidance

https://www.first.org/cvss/v4-0/

2026-09-17 FRESHNESS DELTA

FIRST CVSS remains v4.0; the official specification is document v1.2. CISA KEV and EPSS remain living prioritization inputs.

Freshness policy: scheduled review + immediate review on source supersession, material release, vulnerability, retraction, or contradictory evidence.

Evidence Must Survive Contact With Reality

- Source authority is not implementation evidence. Product behavior, scale, security, interoperability, and operator fit remain environment-specific.
- Conflicting evidence is recorded rather than averaged away. Specification behavior, vendor implementation, preprint results, and production observations are separate evidence classes.
- Quantitative claims are informative until reproduced under documented hardware, software, data, topology, load, and failure conditions.
- Adoption posture is reversible. A stronger source set can coexist with a pilot-only or research-only recommendation when maturity, safety, economics, or operability remain unresolved.

ADOPTION / VALIDATION / REVIEW

Decision Gate and Validation Plan

ADOPTION POSTURE

ADOPT NOW

Adopt a composite prioritization model that combines active exploitation, exploit probability, technical severity, asset exposure, business criticality, compensating controls, and remediation feasibility.

1 / SOURCE	Pin exact versions, publication state, retrieved artifacts, and source hashes.
2 / PROTOTYPE	Demonstrate the core mechanism with representative data and instrumented execution.
3 / FAILURE	Exercise malformed input, dependency loss, stale state, overload, recovery, rollback, and misuse.
4 / BASELINE	Compare against an incumbent, classical, or simpler architecture using the same workload.
5 / ACCEPT	Record acceptance criteria, residual limitations, owner, expiration, and revalidation triggers.

EXPIRATION / REVIEW TRIGGER

Next scheduled review: 2026-12-16 (90-day cadence). Review sooner after material source revision, breaking implementation release, critical vulnerability, retraction, benchmark contradiction, changed workload, or changed legal/safety boundary.

8. Complete Source Research Note

SOURCE-LINEAGE NOTICE

The following material preserves the complete original source note, excluding only the conversational wrapper and outer Markdown fence. Legacy status labels and absolute language are retained for traceability and do not override the candidate status, limitations, or adoption decision in this edition.

Document ID: RES-004 Version: 1.0.0 (Definitive Registry Edition) Status: Published Research Note Classification: Public Organization: Mythos Systems (MYTHOS AI) Owner: Aaron Stovall Effective Date: 2026-07-16 Applies To: Security engineers, vulnerability management teams, and SREs designing patch cadences, SLA bounds, and automated remediation pipelines Companion Standards: MYTHOS-SEC-0008 (Vulnerability Management & Exposure Assessment), MYTHOS-GRC-0001 (Federal & DoD Compliance), MYTHOS-SRE-0001 (SLOs & Error Budgets)

The architecture of vulnerability management has failed. Organizations blindly mandate that "all Critical (CVSS 9.0+) vulnerabilities must be patched within 14 days." This severity-based paradigm is a suicide pact. Security teams spend weekends patching esoteric, local-privilege-escalation bugs on isolated servers (which have a 0.001% chance of being exploited) while ignoring lower-scored (CVSS 7.5) remote code execution vulnerabilities on internet-facing servers that are being actively weaponized by ransomware gangs.

This research note defines the mechanics of Exploitability Prioritization. In a Mythos-compliant architecture, CVSS is merely a technical severity baseline, not a call to action. True prioritization requires the triangulation of three data points:

1. CVSS: How bad is it if exploited?
2. EPSS: How likely is it to be exploited in the next 30 days?
3. CISA KEV: Is it actively being exploited right now?

By mapping these three vectors against asset criticality and exposure, we transform vulnerability management from an alert-fatigue treadmill into a mathematically bounded, risk-driven remediation engine.

To engineer a prioritization model, we must define the exact nature and limitations of each signal.

1.1 CVSS (Common Vulnerability Scoring System)

- What it measures: The technical severity of the vulnerability. It evaluates the exploit method (Network, Local, Adjacent), the impact (Confidentiality, Integrity, Availability), and user interaction requirements.
- The Flaw: CVSS is context-blind. A 9.8 CVSS memory corruption bug means nothing if the vulnerable service is not running, is behind a mTLS gateway, or requires physical access to the machine. Furthermore, CVSS scores are rarely downgraded when mitigations are applied. Treating CVSS as the sole prioritization metric guarantees operational paralysis.

1.2 EPSS (Exploit Prediction Scoring System)

- What it measures: A probabilistic score (0.0 to 1.0) generated by a machine learning model (managed by FIRST.org). It predicts the probability that a specific CVE will be exploited in the wild within the next 30 days.
- The Flaw: EPSS is a statistical prediction based on historical data and threat intelligence feeds. It is highly effective at filtering out "dead" CVEs, but it is not real-time intelligence. A zero-day might have a low EPSS score for the first 48 hours until the model catches up to the new exploit activity.

1.3 CISA KEV (Known Exploited Vulnerabilities)

- What it measures: A deterministic, authoritative catalog maintained by CISA. If a CVE is on this list, it is being actively exploited in the wild right now.
- The Flaw: The KEV catalog is reactive and US-government-focused. It does not capture every niche exploit being used in targeted attacks, and there is a delay between a vulnerability being exploited and CISA adding it to the catalog.

The consequence of ignoring this triad is alert fatigue.

If an organization relies solely on CVSS, a typical enterprise might see 500 "Critical" vulnerabilities a week. The security team cannot patch 500 servers a week. They become desensitized. When a truly catastrophic, internet-facing, actively exploited vulnerability drops (like Log4Shell), it is buried in a queue of 499 irrelevant Criticals.

Conversely, if an organization relies solely on the KEV catalog, they might miss a vulnerability with a 99% EPSS probability that hasn't quite crossed the threshold of CISA's radar yet.

Threat actors explicitly design their initial access brokers to exploit the CVSS bias of enterprise security teams.

3.1 The Niche Exploit (Low CVSS, High EPSS)

An attacker purchases access to a botnet that targets a specific, obscure file-upload vulnerability in a legacy CMS. The CVSS score is 6.5 (Medium) because it requires authentication. However, default credentials for the CMS are public, making the EPSS 0.95 (95% chance of exploitation). The security team ignores the alert because it is not "Critical," and the attacker breaches the network.

3.2 The Chained Exploit

An attacker chains a low-severity information disclosure bug (CVSS 5.3) with a local privilege escalation bug (CVSS 7.1). Neither triggers a critical SLA. The attacker achieves remote code execution (RCE) through the combination, bypassing the severity-based patching queue entirely.

Defending against alert fatigue requires a convergent prioritization engine. The security architecture MUST automatically ingest all three data points and map them against the asset's context (Exposure + Criticality).

4.1 The KEV Velocity Override

If a CVE exists in the CISA KEV catalog, its CVSS and EPSS scores are mathematically irrelevant. It MUST be elevated to the top of the remediation queue.

- Rule: `IF KEV == TRUE -> SLA = 72 Hours` (or less, if internet-facing).

4.2 The EPSS/CVSS Matrix (Risk Quadrants)

For non-KEV vulnerabilities, the system MUST utilize a matrix to determine SLAs:

- High CVSS (> 8.0) + High EPSS (> 0.5): Critical Risk. Patch within 7 days.
- High CVSS (> 8.0) + Low EPSS (< 0.05): Theoretical Risk. Patch within 30 days. (Do not wake up the on-call engineer).
- Low/Med CVSS (< 7.0) + High EPSS (> 0.5): Hidden Risk. Patch within 14 days. (Threat actors are actively targeting this).

4.3 Contextualization (Asset Exposure)

A 9.8 CVSS vulnerability on a server is meaningless without context. The prioritization engine MUST ingest data from the CMDB and Cloud Control Plane:

- `Is the asset internet-facing?`
- `Is the vulnerable port actively listening?`

- `Is the asset in a PCI/HIPAA scoped boundary?`
- Rule: `IF InternetFacing == TRUE -> Reduce SLA by 50%`

4.4 Automated Drift to Known-Safe

When a vulnerability enters the "Critical Risk" quadrant, the system SHOULD not just create a ticket. It MUST trigger a SOAR playbook to automatically isolate the host, block the port at the firewall, or apply a virtual patch via the WAF, buying time for the OS team to apply the actual patch.

The shift from severity-based to exploitability-based vulnerability management is the only mathematically sound way to secure modern infrastructure. By triangulating CVSS (Impact), EPSS (Probability), and KEV (Reality), and mapping them against asset exposure, organizations can drastically reduce Mean Time To Remediate (MTTR) for actual threats while ignoring the noise of theoretical CVEs.

```
CVSS measures the crash; EPSS measures the probability; KEV measures the reality.
A 9.8 behind a firewall is a ghost.
A 6.5 on the internet is a breach.

Severity is a technical characteristic; exploitability is an operational truth.

> Vulnerabilities may be abundant.
> Remediation must be absolute and prioritized.
```

End of Research Note RES-004

9. Source Register

Source	Authority and Status	Freshness Control
CISA Known Exploited Vulnerabilities Catalog https://www.cisa.gov/known-exploited-vulnerabilities-catalog	Primary government operational source Continuously updated Published: Living	Validated: 2026-07-22 Review on material revision, withdrawal, supersession, or scheduled report review.
FIRST EPSS User Guide https://www.first.org/epss/user-guide	Primary scoring-system guidance Living Published: Living	Validated: 2026-07-22 Review on material revision, withdrawal, supersession, or scheduled report review.
FIRST CVSS v4.0 Specification and Guidance https://www.first.org/cvss/v4-0/	Primary scoring standard Current major version Published: 2023	Validated: 2026-07-22 Review on material revision, withdrawal, supersession, or scheduled report review.

10. Lineage, Review, and Publication Record

Record	Value
Original source file	RES-004_CISA_KEV_EPSS_CVSS_Exploitability_Prioritization_Models.md
Original source words	1175
Upgrade type	Enterprise research report; source and freshness validation; limitations; adoption decision; reproducibility plan
Generated on	2026-07-22
Current status	Candidate Research Report
Publication authority	Formal Mythos approval not yet recorded
Next review	90 days or event-driven trigger, whichever occurs first