A Finer Exploitability Gradation (VLEV) for FedRAMP Rev5 VDR/VER

Matthew Venne
Chief Technology Officer, stackArmor

June 2026

Abstract

This is a companion proposal to *A Deterministic, CVSS–Environmental Method for FedRAMP Rev5 VDR/VER Vulnerability Prioritization*, which derives a Potential Agency Impact rating (PAIN, N1–N5) and a VDR-TFR-PVR remediation deadline for each finding. That method treats exploitability as a single yes/no line (Likely-Exploitable or not). This proposal recommends splitting it into *three* bands so the very tightest remediation clocks are reserved for the flaws most likely to be exploited in the wild — and shows that the change is purely additive to the existing remediation matrix, slowing nothing down. The key words MUST, SHOULD, and MAY are to be read as in RFC 2119.

1 The added inflection point

The reference method uses one EPSS cut to separate Likely-Exploitable (LEV) from Not (NLEV). We propose *two* cuts and three bands:

- **NLEV** — EPSS ≤ 0.30: not likely exploitable.
- **LEV** — $0.30 <$ EPSS ≤ 0.75: likely exploitable.
- **VLEV** — EPSS > 0.75: *very* likely exploitable.

Observed active exploitation always maps to VLEV, regardless of EPSS: if CISA Vulnrichment reports `exploitation = active` (KEV-equivalent), the flaw is being used *now* and belongs in the most-urgent band by definition.

2 Alignment with CISA Vulnrichment

The split is not arbitrary — it mirrors the taxonomy of the authoritative source. CISA Vulnrichment's SSVC *Exploitation* metric already distinguishes three states: `none`, `poc` (a public proof-of-concept exists), and `active` (observed in the wild). Today's binary LEV/NLEV flattens that distinction; the proposed bands restore it, with each state lining up to a band and EPSS supplying the statistical estimate where Vulnrichment is silent:

- `none` → NLEV (no known exploit; statistically EPSS ≤ 0.30).
- `poc` → LEV (exploit code exists, not yet widespread; EPSS 0.30–0.75).
- `active` → VLEV (being used now; EPSS > 0.75).

As with `active`→VLEV, a known `poc` state can floor a finding to LEV even when its EPSS is lower. The exploitation *state* (when known) and the EPSS *probability* (always available) then agree on one three-tier scale instead of being forced into a two-way yes/no.

3 Calibration: anchored on today's matrix

We anchor the three bands on FedRAMP's existing deadlines so adoption is trivial and *nothing remediates slower than today*:

- **VLEV reuses FedRAMP's current LEV deadlines, unchanged** — the very-likely / actively-exploited band keeps today's fastest clock.
- **LEV** (the new 0.30–0.75 band) gets *slightly more* time than VLEV — likely, but not certain, so a modest grace over the actively-exploited band, and a large speed-up versus today, where this band sat in the slow NLEV column.
- **NLEV** (≤ 0.30) keeps today's slow deadline as `NLEV+NIRV` and now *splits* by reachability, so a not-likely-but-internet-reachable flaw (`NLEV+IRV`) is modestly tighter than a purely internal one.

Within every band, internet-reachable (IRV) is tighter than not-reachable (NIRV). The result is six remediation columns in place of today's three.

4 The proposed matrix

Tables 1–3 give the full six-column grid per Certification Class (days; 0.5 = 12 hours). Columns are grouped by reachability; within each group the three exploitability bands increase left to right. The VLEV columns and `NLEV+NIRV` reproduce the provider's current matrix exactly; `LEV` and `NLEV+IRV` are the new, faster columns. PAIN-1 carries no FedRAMP deadline. Values are illustrative of a representative VDR-TFR-PVR profile; the authoritative day counts remain FedRAMP's to set.

	Internet-reachable (IRV)			**Not reachable (NIRV)**		
PAIN	VLEV	LEV	NLEV	VLEV	LEV	NLEV
N5	4	6	16	8	12	32
N4	8	12	48	32	48	64
N3	32	48	96	64	96	192
N2	96	144	176	160	192	192

Table 1: Proposed six-column grid — **Class A / B** (days; 0.5 = 12 h).

	Internet-reachable (IRV)			**Not reachable (NIRV)**		
PAIN	VLEV	LEV	NLEV	VLEV	LEV	NLEV
N5	2	3	8	4	6	16
N4	4	6	32	8	12	64
N3	16	24	64	32	48	128
N2	48	72	160	128	160	192

Table 2: Proposed six-column grid — **Class C** (days; 0.5 = 12 h).

	Internet-reachable (IRV)			Not reachable (NIRV)		
PAIN	VLEV	LEV	NLEV	VLEV	LEV	NLEV
N5	0.5	1	4	1	2	8
N4	2	3	16	8	12	32
N3	8	12	48	16	24	64
N2	24	36	160	96	144	192

Table 3: Proposed six-column grid — **Class D** (days; 0.5 = 12 h).

5 Net effect and adoption

Nothing slows down. The actively-exploited / > 0.75 band keeps FedRAMP's current LEV clock; the broad 0.30–0.75 middle band — previously parked in the slow NLEV column — accelerates onto a near-LEV clock; and reachability now refines the not-likely band. Because a conforming implementation already drives remediation from a config-driven `[Class][PAIN][column]` lookup, this is additive: it adds columns, not a redesign. An adopter MAY tune the two EPSS cut points (0.30, 0.75) and the per-Class day counts; the structural recommendation is the three-tier exploitability axis aligned to CISA Vulnrichment's `none`/`poc`/`active` states.