FRAMEWORK #170

Patch Visibility Debt

DEFINITION

Debt accumulates whenever remediation priority depends on confirmation signals that arrive later than attacker activity. KEV listings, public proof-of-concept code, vendor advisories, and threat-intel feed alerts are examples of confirmation signals, not the definition itself.

FRAMEWORK FLOW

01
Exploitation Begins
Attacker activity starts before confirmation exists.

02
Visibility Lags
Available confirmation signals remain behind attacker activity.

03
Priority Discounts
Remediation logic treats the absence of confirmation as lower urgency.

04
Debt Comes Due
Confirmation arrives, exposing that the organization already carried the exposure.

Failure State: Confirmation-Driven Backdating

`Exploitation begins, unconfirmed` → `Priority ranked as low-urgency` →

`Public PoC or advisory surfaces` → `KEV or vendor confirmation lands` →

`Priority decision exposed as wrong from day one`

THE DIAGNOSTIC SIGNAL

SIGNAL OWNERSHIP

Ask any confirmation source whether it accurately reported what it had itself confirmed. Yes, always — source ownership exists at every layer.

EXPOSURE OWNERSHIP

Ask who owns the question of whether exploitation has actually started. Nobody — exposure ownership does not exist. Every source can correctly report what it has confirmed; nobody is assigned to report whether exploitation has already begun.

TRIGGER CONDITION

A remediation policy that ranks urgency by confirmation-source status rather than exposure is the activation condition. Exposure-first policies never trigger the gap.

REMEDIATION SHAPE

Exposure-first prioritization, patch-to-confirmation lag tracked as its own metric, "unconfirmed" and "not occurring" recorded as separate facts — architectural, not procedural.

THE FOUR CONFIRMATION SOURCES

Every signal below is temporally downstream of the event it's meant to help prioritize — what each one tells you is not what it fails to tell you.

THREAT-INTEL FEED ALERT

Tells you someone observed or is reporting activity. Does not tell you that its absence means no exploitation is occurring.

VENDOR ADVISORY

Tells you the vendor has observed or confirmed something on their end. Does not tell you attacker activity hasn't already started elsewhere — "not yet observed exploited" describes vendor visibility, not vulnerability risk.

PUBLIC PROOF-OF-CONCEPT

Tells you exploitation knowledge has become public. Does not tell you exploitation began when the PoC appeared.

KEV CATALOG ADDITION

Tells you CISA has independently confirmed and cataloged exploitation. Does not tell you exploitation began when KEV listed it — confirmation is gated on evidence reaching CISA first, making it inherently downstream of the underlying event.

ARCHITECTURAL RELATIONSHIPS

#162
Security Entropy Accumulation

RELATED · MODERATE

Same "you think you're fine but you're not" family from a different angle — #162 is posture decaying silently despite configuration convergence; #170 is organizations staying behind attacker activity despite active monitoring.

ANCHOR /patch-visibility-debt/

TRIGGERING EXAMPLE

Domain- and vendor-agnostic beyond this anchor — the same shape recurs across Exchange, Citrix, Fortinet, VMware, identity providers, and AI control planes.

"Every confirmation source can correctly report what it has itself confirmed. Nobody can report whether exploitation has already started — not because anyone neglected it, but because no single source was ever assigned that job."