INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-10 18:37 UTC

Patch Lag Is Structural, Not Operational: One Billion KEV Records Confirm Human-Scale Defense Has Hit Its Ceiling

SECURITY ANALYSIS | HIGH | CVSS 7.5

SCC Item ID	SCC-STY-2026-0053
Type	Security Analysis
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Broad enterprise environments; study references Spring4Shell (CVE-2022-22965), Cisco IOS XE, Follina (CVE-2022-30190) as illustrative high-profile cases; 10,000 organizations in Qualys TRU dataset
Published	2026-04-10T10:01:11
Discovery Source	Rss

Executive Summary

A Qualys Threat Research Unit analysis of over one billion CISA KEV remediation records across 10,000 organizations reveals that attackers are exploiting high-profile vulnerabilities an average of seven days before enterprises even begin remediation. Despite organizations closing roughly 400 million more vulnerability events annually, the share of critical vulnerabilities still open at Day 7 post-disclosure has worsened from 56% to 63%, indicating that doing more of the same is not closing the gap. The study signals a structural inflection point: the traditional scan-ticket-patch workflow has reached a ceiling that cannot be resolved through hiring, overtime, or incremental process improvement alone.

Technical Analysis

The Qualys TRU study draws on one billion remediation records from the CISA Known Exploited Vulnerabilities catalog, spanning 10,000 organizations and multiple years of patching activity. The headline finding is a negative Time-to-Exploit (TTE) average of minus seven days, meaning that for high-profile weaponized vulnerabilities, exploitation in the wild precedes the point at which most enterprises have completed, or in many cases initiated, their remediation cycles. This is not an outlier phenomenon. Three illustrative cases anchor the finding. Spring4Shell (CVE-2022-22965), a critical Spring Framework remote code execution flaw scored 9.8 CVSS by NVD, saw active exploitation emerge within days of public disclosure in March 2022, before most enterprise patch cycles had advanced past detection. Follina (CVE-2022-30190), a Microsoft MSDT RCE flaw

(MITRE T1203, T1190), was actively exploited as a zero-day for a period before Microsoft released a patch. The Cisco IOS XE authentication bypass reached weaponization while tens of thousands of internet-exposed devices awaited remediation. The throughput paradox embedded in the data is the more analytically significant finding. Organizations are closing more vulnerabilities in absolute terms, yet the 7-day open rate for critical flaws has climbed from 56% to 63%. This divergence reflects a structural dynamic: as vulnerability disclosure volume grows, triage and prioritization bottlenecks compound faster than remediation capacity scales. The scan-ticket-patch model, which depends on human review at each handoff, does not compress cycle time proportionally with added headcount. The MITRE techniques most directly implicated across the referenced cases include T1190 (Exploit Public-Facing Application), T1068 (Exploitation for Privilege Escalation), T1203 (Exploitation for Client Execution), and T1588.006 (Obtain Capabilities: Vulnerabilities), reflecting a consistent attacker pattern of acquiring and weaponizing disclosed flaws before defenders complete remediation. CWE classifications in the dataset (CWE-119 (Buffer Overflow), CWE-693 (Protection Mechanism Failure), CWE-20 (Improper Input Validation), and CWE-269 (Improper Assignment of Privileged Status)) suggest the underlying flaw categories remain durable attacker targets that have resisted elimination across successive software generations. The study's conclusion is direct: the deficit is not operational, it is architectural. Faster ticket routing and additional scanning cycles will not close a gap that originates in the structural latency of human-gated workflows.

Action Checklist

1. Step 1: Assess exposure, audit your organization's current open vulnerability backlog against the CISA KEV catalog; identify any items older than seven days that remain unremediated, as the TRU data places these in the highest-risk cohort
2. Step 2: Review controls, verify that network segmentation, EDR coverage, and exploit prevention controls (application allowlisting, memory protection) are active on systems hosting public-facing applications (T1190) and client-facing software (T1203); compensating controls must cover the gap when patching is delayed
3. Step 3: Update threat model, incorporate negative-TTE exploitation patterns as a standing assumption; treat KEV-listed vulnerabilities as probable targets for active exploitation within the first 7 days post-disclosure, even before exploitation is widely reported
4. Step 4: Evaluate workflow architecture, assess whether your current vulnerability management pipeline has human-gated handoffs that structurally prevent sub-7-day remediation for critical flaws; identify which steps (triage, approval, change management) can be automated or pre-authorized for KEV-class findings
5. Step 5: Communicate findings, brief leadership on the throughput paradox: closing more vulnerabilities annually while the 7-day critical open rate worsens requires a strategic, not operational, response; frame this as a resourcing model question, not a team performance issue
6. Step 6: Monitor developments, track Qualys TRU publication updates and CISA KEV additions for new entries with negative or near-zero TTE histories; these represent your highest-priority remediation targets

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to CISO and legal counsel immediately if any asset in the KEV backlog older than 7 days is confirmed internet-facing and running a service matching the Qualys TRU high-profile cases (Spring Framework apps on CVE-2022-22965, Office/MSDT-enabled endpoints on CVE-2022-30190, or Cisco IOS XE web UI on CVE-2023-20198/CVE-2023-20273), or if regulatory obligations apply (SEC 4-day cyber disclosure rule, HIPAA breach notification, PCI DSS Requirement 6.3) and exploitation cannot be ruled out.
Recovery Notes	After remediating KEV-backlogged items, do not close the incident ticket until you have verified patch deployment via authenticated scanner confirmation (not just ticket closure) and reviewed the 30-day window of web server access logs, EDR telemetry, and authentication logs for indicators consistent with pre-patch exploitation — specifically, web shell artifacts in the Spring4Shell-affected application directories, anomalous MSDT/sdiagnhost.exe process trees on Office endpoints, and unauthorized account creation in Cisco IOS XE privilege-15 accounts. Maintain elevated monitoring on previously-exposed systems for 90 days post-patch, given that threat actors exploiting negative-TTE vulnerabilities frequently establish persistence before defenders begin remediation, making the patch itself insufficient to confirm clean state.
Forensic Artifacts	CISA KEV JSON feed diff exports with timestamps (cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json): records which KEV CVEs were added and when, establishing the organizational awareness timeline for regulatory and legal review | Web server access logs (Apache access.log, Nginx access.log, IIS W3C logs) filtered for Spring4Shell exploit patterns ('class.classLoader', 'class.module.classLoader', 'suffix=.jsp') and Cisco IOS XE path traversal patterns used in the 2023 web UI exploitation campaign | Windows Security Event Log Event ID 4688 (Process Creation) and Event ID 4104 (PowerShell Script Block) on Office-suite endpoints: filter for msdt.exe or sdiagnhost.exe with parent processes winword.exe, excel.exe, or outlook.exe — the canonical Follina/CVE-2022-30190 execution chain | Vulnerability scanner historical scan reports (Qualys, Tenable, OpenVAS) with first-seen date and remediation-verified date for each KEV CVE: this delta constitutes your organization-specific time-to-remediation evidence and is required for post-incident regulatory disclosure accuracy | Cisco IOS XE 'show users', 'show running-config | section ip http', and syslog entries for unexpected privilege-15 account creation or HTTP server access from non-management IPs — artifacts consistent with the implant-stage activity observed in the 2023 Cisco IOS XE mass exploitation campaign tracked by Censys and VulnCheck

Per-Action IR Details

Step 1: Assess exposure — audit your organization's current open vulnerability backlog against the CISA KEV catalog; identify any items older than seven days that remain unremediated, as the TRU data places these in the highest-risk cohort

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: establishing situational awareness and vulnerability posture as a precondition to effective incident handling

Controls: NIST SI-2 (Flaw Remediation), NIST RA-5 (Vulnerability Monitoring and Scanning), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Export the CISA KEV catalog JSON from https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json and cross-reference it against your asset inventory using a two-command PowerShell pipeline: (1) pull installed software/patch state via 'Get-HotFix' and 'Get-WmiObject Win32_Product', (2) compare CVE fields against KEV entries with a Python diffing script. For Linux hosts, run 'apt list --installed' or 'rpm -qa' piped into a grep loop against KEV CVE IDs. Flag any KEV entry where

'dateAdded' is more than 7 days ago and the patch is not confirmed applied.

Evidence: Before remediating, snapshot the current vulnerability state as forensic baseline: export the full Qualys/Tenable/OpenVAS scan report (or 'wmic qfe list' output on Windows) with timestamps to establish which KEV-listed CVEs — specifically Spring4Shell (CVE-2022-22965) on Spring Framework deployments, Follina (CVE-2022-30190) on Office/MSDT-enabled endpoints, and Cisco IOS XE web UI CVEs on network edge devices — were open and for how long; this timestamped export is your evidence of exposure duration if a breach is later confirmed.

Step 2: Review controls — verify that network segmentation, EDR coverage, and exploit prevention controls (application allowlisting, memory protection) are active on systems hosting public-facing applications (T1190) and client-facing software (T1203); compensating controls must cover the gap when patching is delayed

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: ensuring defensive tools and network architecture can limit blast radius during the exploitation window that precedes patch completion

Controls: NIST SC-7 (Boundary Protection), NIST SI-3 (Malicious Code Protection), NIST SI-4 (System Monitoring), NIST IR-4 (Incident Handling), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: For T1190 (public-facing application exploitation, as with Spring4Shell and Cisco IOS XE): deploy ModSecurity with the OWASP Core Rule Set in front of any Java Spring or web application server to detect class.classLoader and Runtime.exec() payload patterns characteristic of Spring4Shell; rule CRS 944130 specifically targets Spring Framework RCE attempts. For T1203 (client-side exploitation, as with Follina/CVE-2022-30190): deploy Sysmon with SwiftOnSecurity's config and enable Event ID 4688 process creation auditing; write a Sigma rule detecting msdt.exe or sdiagnhost.exe spawned by winword.exe, excel.exe, or outlook.exe — this process chain is the Follina execution fingerprint. Use Windows Defender Application Control (WDAC) or AppLocker in audit mode to enumerate unsigned binary executions before enforcing.

Evidence: Capture current EDR coverage gap data before tuning: on Windows hosts, run 'Get-Service -Name sense,windefend' and 'sc query diagtrack' to confirm Defender/MDE sensor status; on Linux, verify auditd ruleset with 'auditctl -l' and confirm rules exist for execve syscalls on web server process trees (e.g., java, python, php-fpm); for Cisco IOS XE edge devices, pull the running config and verify access-class restrictions on the HTTP/HTTPS server — 'show running-config | section ip http' — and confirm whether the web UI (exploited in 2023 Cisco IOS XE campaign, CVE-2023-20198/CVE-2023-20273) is disabled or IP-restricted.

Step 3: Update threat model — incorporate negative-TTE exploitation patterns as a standing assumption in your threat model; treat KEV-listed vulnerabilities as actively exploited by default from the moment of disclosure, not after confirmed in-the-wild reports reach your team

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: refining detection criteria and incident declaration thresholds to reflect attacker timelines that outpace organizational response cycles

Controls: NIST RA-3 (Risk Assessment), NIST IR-8 (Incident Response Plan), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Operationalize the negative-TTE assumption without a threat intelligence platform by creating a standing CISA KEV RSS/JSON monitor using a free cron job or GitHub Actions workflow that polls the KEV feed daily, diffs new entries against your asset inventory, and fires a Slack/email alert; treat every new KEV addition as an active incident triage ticket on Day 0, not Day 7. Map each KEV entry to MITRE ATT&CK technique IDs (T1190 for network-facing services, T1203 for client software) to pre-stage detection logic in Sysmon and Sigma rules before exploitation is confirmed in your environment.

Evidence: Document the threat model update itself as an artifact: record the KEV catalog version hash and date, the list of affected assets mapped to each KEV CVE, and the MITRE ATT&CK technique assignments — this creates an auditable decision trail showing when your organization recognized the active exploitation risk, which is material evidence in post-incident regulatory inquiries (e.g., SEC cyber disclosure, HIPAA breach investigation) asserting whether the risk was known and unaddressed.

Step 4: Evaluate workflow architecture — assess whether your current vulnerability management pipeline has human-gated handoffs that structurally prevent sub-7-day remediation for critical flaws; identify which steps (triage, approval, change management) can be automated or pre-authorized for KEV-class findings

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: building response infrastructure and pre-authorization frameworks that compress time-to-remediation below the attacker exploitation window identified in the Qualys TRU dataset

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-2 (Flaw Remediation), NIST CM-3 (Configuration Change Control), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Map your current patch pipeline on a whiteboard with timestamps at each handoff (scan → ticket creation → triage → approval → maintenance window → deployment → validation); measure the cumulative delay against the 7-day TTE threshold from the Qualys TRU data. For KEV-class findings, draft a pre-authorization policy that grants the security team a standing change window (e.g., 4-hour emergency window, any day) for CVSS ≥ 9.0 KEV entries — eliminating the CAB approval handoff for this specific class. Automate patch deployment for Windows KEV targets using WSUS or PDQ Deploy with a KEV-triggered job; for Linux, use unattended-upgrades with a curated security-only source list.

Evidence: Before restructuring the pipeline, extract workflow timing data as evidence of structural lag: pull ticket timestamps from your ITSM (ServiceNow, Jira, or even a spreadsheet log) for the last 10 KEV-listed CVEs your team remediated, recording time from CVE KEV-addition date to patch-verified-deployed date; this delta data, compared against the Qualys TRU 7-day benchmark, constitutes your risk acceptance documentation and justifies the architectural change to leadership and auditors.

Step 5: Communicate findings — brief leadership on the throughput paradox: closing more vulnerabilities annually while the 7-day critical open rate worsens requires a strategic, not operational, response; frame this as a resourcing model question, not a team performance issue

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: lessons learned and organizational feedback loops that translate technical findings into leadership-level structural improvements

Controls: NIST IR-6 (Incident Reporting), NIST IR-8 (Incident Response Plan), NIST PM-1 (Information Security Program Plan), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Build the leadership brief around three data points drawn directly from the Qualys TRU findings: (1) your organization's current KEV backlog count and average age of open critical items, (2) your annual vulnerability closure count year-over-year to demonstrate the throughput paradox is real in your environment, and (3) the percentage of your KEV-listed items that were open beyond Day 7 post-disclosure. Use a free data visualization tool (Google Sheets, LibreOffice Calc, or the Python matplotlib library) to plot vulnerability closure volume alongside 7-day open rate on a dual-axis chart — this makes the paradox visually undeniable for non-technical executives.

Evidence: The evidentiary package for this brief is your organization's own patch timing data: export from your vulnerability scanner (Qualys, Tenable, or OpenVAS) the first-seen date, KEV-addition date, and remediation-verified date for every KEV CVE in the last 12 months; the gap between KEV-addition date and remediation-verified date, averaged across the dataset, is your organization-specific version of the Qualys TRU 7-day finding — and constitutes audit-ready evidence of systemic risk that leadership is now formally informed of.

Step 6: Monitor developments — track Qualys TRU publication updates and CISA KEV additions for new entries with negative or near-zero TTE histories; these represent your highest-priority remediation targets

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: continuous monitoring and threat intelligence integration to identify emerging KEV entries with pre-disclosure exploitation histories before they manifest as active incidents in the environment

Controls: NIST SI-5 (Security Alerts, Advisories, and Directives), NIST SI-4 (System Monitoring), NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Stand up a free KEV monitoring pipeline using three components: (1) a daily cron job that downloads the CISA KEV JSON feed and diffs it against yesterday's snapshot, outputting net-new entries with their 'dateAdded' and 'knownRansomwareCampaignUse' fields; (2) a Python script that cross-references net-new CVE IDs against NVD's API (free, no key required for basic queries) to pull CVSS score and CWE type; (3) a Shodan free-tier search or Censys Community search to check whether your organization's internet-facing IP ranges are running the affected product/version identified in the new KEV entry. For each net-new KEV entry flagged as high-priority, immediately run a targeted Nessus Essentials (free for up to 16 IPs) or OpenVAS scan scoped to the specific CVE plugin ID.

Evidence: When a new KEV entry is identified — particularly one referencing a product class matching the Spring4Shell (Java Spring apps), Follina (Office/MSDT on Windows endpoints), or Cisco IOS XE (network edge) profiles — immediately capture: (1) web server access logs filtered for exploit-characteristic URI patterns (e.g., 'class.classLoader' or 'class.module.classLoader' in Spring4Shell scans, '?%2F' path traversal patterns in Cisco IOS XE exploitation), (2) Windows Event ID 4104 (PowerShell Script Block Logging) and Event ID 4688 (Process Creation) on Office-suite hosts for Follina-pattern MSDT invocations, and (3) a current Shodan/Censys snapshot of your internet-facing attack surface for the newly KEV-listed product — this establishes a pre-exploitation baseline if the vulnerability is subsequently confirmed exploited in your environment.

Detection Guidance

Because exploitation is occurring before remediation cycles complete, detection must function as the primary control layer during the patching gap. For public-facing application exploitation (T1190): review web application and load balancer logs for unexpected HTTP methods, unusual parameter lengths, or serialization patterns targeting Spring Framework endpoints; alert on POST requests to /actuator paths or class.module.classLoader patterns associated with Spring4Shell. For MSDT and client-execution vectors (T1203, Follina): monitor for winword.exe, outlook.exe, or other Office processes spawning child processes such as msdt.exe, cmd.exe, or PowerShell with encoded arguments; these parent-child chains are anomalous and should alert at high confidence. For privilege escalation post-exploitation (T1068): hunt for unexpected local privilege elevation events, token manipulation, or service installation by non-administrative users in the hours following any high-profile CVE disclosure. For vulnerability acquisition patterns (T1588.006): monitor threat intelligence feeds and dark web-adjacent sources for exploit kit updates referencing your technology stack; a KEV addition combined with a new Metasploit module or PoC commit is a reliable signal to accelerate remediation. Policy gap to audit: verify that your change management process includes a pre-authorized emergency patch track for KEV-listed critical vulnerabilities; if all critical patches require standard change board cycles, the structural latency identified in the TRU study is present in your environment by design.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`Pending — refer to Qualys TRU study and associated BleepingComputer reporting for any published indicators`	The Qualys TRU analysis is a large-scale remediation data study rather than a campaign attribution report; no specific threat-actor IOCs (hashes, IPs, domains) were published in the source material reviewed. Indicators for the referenced illustrative cases (Spring4Shell CVE-2022-22965, Follina CVE-2022-30190, Cisco IOS XE) are available in vendor-specific advisories from Qualys, Rapid7, and Palo Alto Unit 42.	LOW

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1068** — Exploitation for Privilege Escalation
- **T1203** — Exploitation for Client Execution
- **T1588.006** — Vulnerabilities

NIST-800-53R5

- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-6** — Least Privilege
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-16** — Memory Protection
- **SI-10** — Information Input Validation
- **IA-2** — Identification and Authentication (Organizational Users)

OWASP-TOP10-2021

- **A03:2021** — Injection
- **A01:2021** — Broken Access Control

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control

- **6.3** — Require MFA for Externally-Exposed Applications
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

ISO-27001-2022

- **A.8.26** — Application security requirements
- **A.8.8** — Management of technical vulnerabilities
- **A.5.23** — Information security for use of cloud services

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1203	Exploitation for Client Execution	Execution
T1588.006	Vulnerabilities	Resource-Development

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/analysis-of-one-bill...	T3
Spring Framework Zero-Day Remote Code Execution (Spring4Shell ...	https://blog.qualys.com/vulnerabilities-threat-research/2022/03/31/...	T3
CVE-2022-22965 Detail - NVD	https://nvd.nist.gov/vuln/detail/cve-2022-22965	T1
Spring4Shell: Zero-Day Vulnerability in Spring Framework - Rapid7	https://www.rapid7.com/blog/post/2022/03/30/spring4shell-zero-day-v...	T3
CVE-2022-22965 (SpringShell): RCE Vulnerability Analysis and ...	https://unit42.paloaltonetworks.com/cve-2022-22965-springshell/	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-04-10 18:37 UTC by TJS Security Command Center