

Your CVEs

Paste CVE IDs in column A (CVE-YYYY-NNNN). Yellow = you type. Everything to the right fills in.

CVE	Asset / system	Asset criticality	Internet-facing?	Found on	EPSS (optional, if not in KEV)	Fixed on	In KEV?	Vendor · product	Ransomware	EPSS used	Tier	Due	Status	Days left
CVE-2026-65660	intranet-portal	High	Yes	2026-09-21	0.27		Yes	Microsoft · SharePoint		0.021	P1	2026-09-28	Overdue	-4
CVE-2021-44228	billing-api	High	Yes	2026-09-21			Yes	Apache · Log4j2	Known	1.000	P1	2026-09-28	Overdue	-4
CVE-2023-4966	vpn-gw-01	High	Yes	2026-09-21			Yes	Citrix · NetScaler ADC and NetScaler	Known	1.000	P1	2026-09-28	Overdue	-4
CVE-2024-3400	fw-edge-02	High	Yes	2026-09-21			Yes	Palo Alto Networks · PAN-OS	Known	1.000	P1	2026-09-28	Overdue	-4
CVE-2019-0708	legacy-rdp	Medium	No	2026-09-21			Yes	Microsoft · Remote Desktop Services	Known	1.000	P1	2026-09-28	Overdue	-4
CVE-2025-99999	build-runner	Medium	No	2026-09-21			No			0.270	P3	2026-10-21	Open	19
CVE-2022-22965	orders-svc	Medium	No	2026-09-21			Yes	VMware · Spring Framework		0.996	P2	2026-10-05	Open	3
CVE-2024-12345	laptop fleet	Low	No	2026-09-21			No				P4	2026-12-20	Open	79
CVE-2023-34362	file-transfer	High	Yes	2026-09-21			Yes	Progress · MOVEit Transfer	Known	0.999	P1	2026-09-28	Overdue	-4
CVE-2020-1472	dc-01	High	No	2026-09-21		2026-09-25	Yes	Microsoft · Netlogon	Known	0.994	P1	2026-09-28	Fixed	
CVE-2025-11111	wiki	Low	No	2026-09-21			No				P4	2026-12-20	Open	79
CVE-2018-13379	vpn-gw-old	High	Yes	2026-09-21			Yes	Fortinet · FortiOS	Known	1.000	P1	2026-09-28	Overdue	-4

Patch priority dashboard

KEV snapshot 2026.10.01 · EPSS 2026-10-01 · as of 2026-10-02

CVEs in your list	12
Known exploited (in KEV)	9
...of which ransomware-linked	7
Overdue	7
Fixed	1

Tier	Open	Overdue	Fixed
P1	0	7	1
P2	1	0	0
P3	1	0	0
P4	2	0	0

Catalog facts (from the bundled snapshot)

CVEs in KEV	1731
Added in the last 365 days	309
Ransomware-linked	361
Median EPSS of KEV CVEs	0.49

Why KEV first

Scanners report thousands of CVEs, and most will never be used against anyone. CISA's KEV catalog lists the ones with **evidence of exploitation in the wild**. FIRST's EPSS estimates the **probability of exploitation in the next 30 days** for every published CVE. Together they answer the only question a small team has time for: what do we fix first?



EPSS of known-exploited CVEs

EPSS band	KEV CVEs
≥ 0.9	461
0.5-0.9	398
0.1-0.5	418
0.01-0.1	391
< 0.01	62

EPSS is a probability for the next 30 days, so some exploited CVEs score low (old, niche or targeted). That is why KEV membership, not the EPSS number alone, puts a CVE in the top tiers of this playbook.

The four tiers

Tier	Rule	Fix within
P1 • Fix now	In KEV and any of: ransomware-linked, internet-facing asset, high-criticality asset	7 days
P2 • Fix fast	In KEV	14 days
P3 • Plan	Not in KEV, EPSS ≥ 0.1 (10%)	30 days
P4 • Routine	Everything else	next normal patch cycle (≤ 90 days)

Why these numbers? CISA gives US federal agencies a due date with every KEV entry: for the 309 CVEs added in the last 12 months the median was 14 days after being added (range 2-21). 7 and 14 days keep you at or ahead of that pace. Adjust them in the workbook's Policy tab to match your team, then write the numbers down and stick to them.

Asset criticality, in one minute

High: customer data, identity (directories, SSO), remote access (VPN, gateways), money movement, anything internet-facing. **Medium:** internal business systems. **Low:** isolated or easily rebuilt machines.

When you can't patch in time

1. Apply the vendor's mitigation or workaround (often published with the advisory).
2. Reduce exposure: take it off the internet, restrict to VPN or an allow-list, disable the vulnerable feature.
3. Watch it: extra logging/alerts on that system until fixed.
4. Record an exception: who approved it, why, the compensating control and a new date.

A 30-minute weekly routine

1. **Monday, 10 min:** export open findings from your scanner (CVE IDs + asset). Paste into the Prioritizer's Your CVEs tab.
2. **Read the Dashboard:** P1 and P2 counts, anything overdue, ransomware-linked items.
3. **Assign:** every P1 gets an owner and a change ticket today; P2 this week.
4. **Check new KEV additions** (CISA publishes most weeks): does any match your products? If yes it is P1/P2 immediately, whatever the scanner says.
5. **Friday, 10 min:** mark fixed items, update exceptions, note the numbers below.

Five numbers to report each month

Metric	Why it matters
Open KEV CVEs on your assets	The exposure attackers already know how to use
P1/P2 fixed within target (%)	Whether the policy is real
Median days to fix P1	Speed on what matters most
Overdue items with an approved exception	Accepted risk, written down
Internet-facing assets with any open KEV CVE	The front door

Where the data comes from (free)

KEV: CISA's catalog (JSON/CSV feed on [cisa.gov](#)). EPSS: FIRST's daily scores and API ([first.org/epss](#)). Keyscope publishes the same data refreshed daily as an API and a weekly brief if you want it fresh without the spreadsheet.