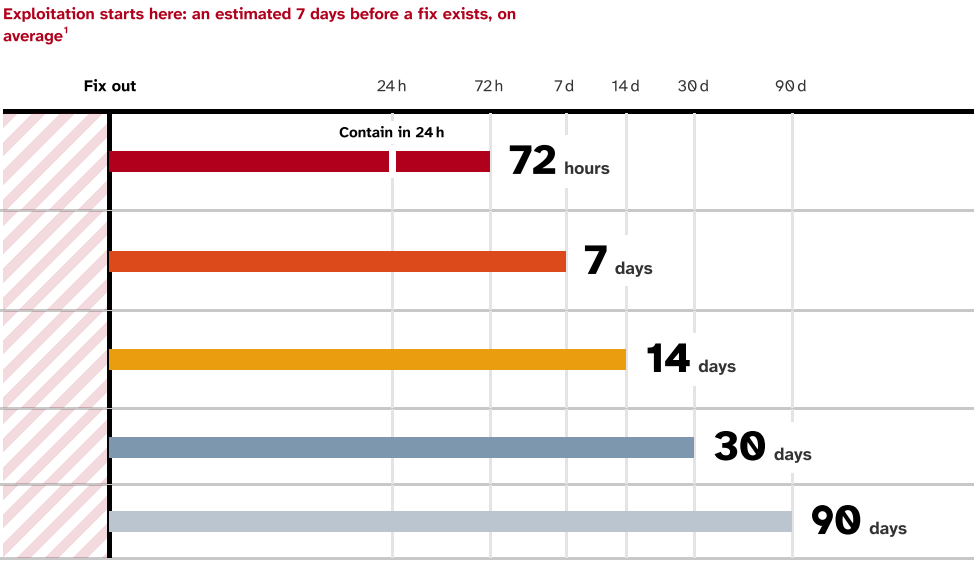
Patching: how fast is fast enough?

If a vulnerability is being exploited and the system is reachable from the internet, contain it within 24 hours and patch within 72. Schedule everything else by exploitation and exposure, not by CVSS score alone.

Reviewed	Next review	Version	Written for	Latest version
5 Nov 2026	**5 Dec 2026**	**1.2**	**IT and security teams of any size**	**sheets.einblick.dev/patching/**

Patch deadlines by risk

Our recommended deadlines, counted from when a fix or official workaround is released. Use the first tier that matches.



Exploited and exposed
Known exploited, on a system reachable from the internet. Edge devices first.

Exploited, internal
Known exploited, reachable only from inside your network.

Exposed and severe
Critical or high severity, or a high EPSS score, on an internet-facing system. No known exploitation.

Internal and severe
Critical or high severity on internal systems.

Everything else
Medium and low severity, no known exploitation.

Log scale. Of the 884 vulnerabilities VulnCheck first saw exploited in 2025, 29% were exploited on or before the day their CVE was published[2], so the first tier starts with containment. For comparison, from December 2026 CISA's BOD 26-04 requires US federal agencies to fix the highest-risk cases within 3 days and any other known-exploited flaw within 14 days[3]; PCI DSS allows 1 month for critical patches[4].

If you only do five things

1. **Know what faces the internet.**
   Keep a live inventory of internet-facing systems. A 72-hour deadline is useless on a server nobody knows about.
2. **Track exploitation, not just severity.**
   Exploitation is now the top initial access vector, at 31% of breaches with a known vector, excluding errors and misuse[5]. Subscribe to CISA KEV[6] and to the advisories of every product you expose.
3. **Patch edge devices first.**
   Security and networking products were hit by 21 of the 43 zero-days aimed at enterprise technology in 2025[7]. If the flaw was exploited, also check them for compromise.
4. **Automate the routine.**
   Enforce automatic updates for operating systems, browsers and apps centrally, so people can focus on the few urgent cases.
5. **Pre-approve the emergency path.**
   Decide in advance who may patch or isolate a system outside the change window, so the 72 hours aren't spent waiting for a meeting.

Triage a new vulnerability

1. **Is it being exploited?**
   Check CISA KEV[6], the vendor advisory and your national CERT. Vendor wording like "limited, targeted exploitation" counts as yes.
2. **Can it be reached from the internet?**
   Check your external inventory. VPNs, firewalls, gateways, mail and file-transfer systems count as exposed by default.
3. **What breaks if it's compromised?**
   Identity systems, edge devices, backups and anything holding customer data move up one tier.
4. **How likely is exploitation soon?**
   For everything else, use EPSS[8] to break ties and recheck weekly. Then record the tier, the deadline and one named owner.

What changed in 2026

- **CISA replaced BOD 22-01** with BOD 26-04 in June 2026. From December 2026, federal deadlines depend on exposure, exploitation, automatability and impact, and the highest-risk cases get 3 days[3].
- **NVD stopped enriching every CVE.** Since April 2026 it prioritizes KEV entries, software the US government uses and critical software[9]. Take severity from the vendor or CNA, and combine it with KEV and EPSS.
- **EPSS moved to version 5** on 15 June 2026[8]. Recheck any score thresholds you tuned on older versions.
- **EU reporting duties for manufacturers started** on 11 September 2026 under the Cyber Resilience Act[10].

Can't make the deadline?

- **Cut the exposure.** Put the system behind a VPN or an IP allowlist, or switch off the vulnerable feature.
- **Apply the vendor's workaround** and write down when it stops being acceptable.
- **Watch the attack path.** Add WAF or IPS rules and alerts for the known exploit.
- **Give the exception an end date.** An accepted risk has a named owner and expires.

What you can skip

- **Sorting by CVSS alone.** It rates severity, not whether anyone is exploiting the flaw. Most published vulnerabilities are never exploited.
- **Chasing zero findings.** Medium and low findings on internal systems belong in the regular cycle. Track deadlines met per tier, not the total open count.
- **Emergency patching every headline.** If it isn't exploited and isn't exposed, it goes in the regular cycle.
- **Long scan reports.** A one-page list of overdue first- and second-tier items does more than a 300-page export.

Mistakes that cost the most

- **Patching without restarting.** Many fixes aren't live until the service or device restarts.
- **Stopping at the patch.** Patching won't remove an attacker who is already in. On exploited edge devices, check the vendor's indicators of compromise, rotate credentials the device handled and review logs from before the patch.
- **Forgetting what scanners miss.** Appliance firmware, container base images and libraries bundled inside other products.
- **Reporting averages.** A good average can hide the one VPN that stayed unpatched for 6 weeks. Report the slowest cases.
- **No owner for vendor-run systems.** If a supplier operates it, the patch deadline belongs in the contract.

What this looks like at your size

Small team, no security staff

- Enforce automatic updates from device management.
- Where you can, use cloud services instead of self-hosted VPNs and gateways, so the provider patches the edge.
- Subscribe to advisories for the few products that face the internet.
- Name one person who owns patching, plus a backup.

Growing, with IT or security staff

- Keep an external attack-surface inventory that updates itself.
- Enrich scanner findings with KEV and EPSS.
- Write down your tiers and deadlines and get them signed off.
- Get an emergency change path pre-approved.

Enterprise or regulated

- Report deadlines met per tier to leadership every month.
- Run risk acceptance with owners and expiry dates.
- Put patch deadlines and advisory duties into supplier contracts.
- Map your tiers to NIS2, DORA or PCI DSS, and keep a compromise-assessment playbook for edge devices.

A separate clock: EU reporting

These run alongside your patch deadline and can start the moment you learn a flaw is being exploited.

Cyber Resilience Act

Manufacturers, for actively exploited vulnerabilities in their own products. Applies since 11 September 2026; reports go through ENISA's Single Reporting Platform[10,11].

24 hours
Early warning

72 hours
Vulnerability notification

14 days
Final report, counted from when a fix or mitigation is available

NIS2

Essential and important entities, for significant incidents[12]. NIS2 sets no patch deadline; its implementing rules for digital service providers ask only for patches "within a reasonable time"[13]. A signed-off tier table shows what reasonable means for you.

24 hours
Early warning

72 hours
Incident notification

1 month
Final report, counted from the notification

Measure the right things

- **Deadlines met per tier.** Aim for 100% on the first tier.
- **Oldest open known-exploited vulnerability.** Track its age in days.
- **Time from advisory to decision.** Slow triage eats the deadline before anyone patches.
- **Coverage.** The share of systems reporting to your patch and scanning tools. Systems you can't see never show up as overdue.

Version history

5 Nov 2026, version 1.2 Stated the scope of the DBIR's 31% figure: breaches with a known initial access vector, excluding errors and misuse.

Sources

1. M-Trends 2026: Data, Insights, and Strategies From the Frontlines. Google Cloud (Mandiant), 23 Mar 2026. cloud.google.com
2. VulnCheck State of Exploitation 2026. VulnCheck, 21 Jan 2026. vulncheck.com
3. BOD 26-04: Prioritizing Security Updates Based on Risk. CISA, 10 Jun 2026. cisa.gov
4. FAQ 1597: Assigning risk rankings to vulnerabilities and resolving them (requirement 6.3.3). PCI Security Standards Council, May 2025. pcisecuritystandards.org
5. 2026 Data Breach Investigations Report. Verizon, 19 May 2026. verizon.com
6. Known Exploited Vulnerabilities Catalog. CISA, 1,766 entries on 30 Oct 2026. cisa.gov
7. Look What You Made Us Patch: 2025 Zero-Days in Review. Google Threat Intelligence Group, 5 Mar 2026. cloud.google.com
8. EPSS: Get the data. FIRST, version 5 since 15 Jun 2026. first.org
9. NIST Updates NVD Operations to Address Record CVE Growth. NIST, 15 Apr 2026. nist.gov
10. Regulation (EU) 2024/2847 (Cyber Resilience Act), Articles 14 and 71. EUR-Lex, 2024. eur-lex.europa.eu
11. The CRA Single Reporting Platform is launched. ENISA, 11 Sep 2026. enisa.europa.eu
12. Directive (EU) 2022/2555 (NIS2), Article 23. EUR-Lex, 2022. eur-lex.europa.eu
13. Implementing Regulation (EU) 2024/2690, Annex point 6.6. EUR-Lex, 2024. eur-lex.europa.eu