CVE Analysis Report

1 January – 22 September 2026 · what was published, what is being exploited, and what has a public exploit

GENERATED 2026-09-22 07:52 UTC · DATA FROM NVD, FIRST EPSS, CISA KEV AND EXPLOIT-DB, REFRESHED DAILY

70,686
CVEs published this year
14,081 in the last 30 days, 4,328 in the last 7

233
added to CISA KEV this year
1,717 in the catalogue in all

172
gained a public exploit this year
25,049 CVEs with an Exploit-DB entry in all

316
new this year with EPSS 10%+
one in ten chance of exploitation within 30 days

81
vendors with a CVE this year
as named in NVD's product data

395,963
CVEs in the explorer
since 1999

So far in 2026, 70,686 vulnerabilities have been published, 8,060 of them rated critical. Of those, 161 (0.2%) are known to be exploited according to CISA, and 172 have a working exploit published in Exploit-DB. That is the whole point of this report: the volume is large, the part that needs an emergency change is small, and the data tells you which is which.

Read it in this order. The heatmaps on the next page show where the year's CVEs sit by month, severity and exploitability; the treemap shows which vendors carry the volume; the radial histogram and the beeswarm show the rhythm of publication and how the exploited minority scores. The tables that follow are the CVEs to check against your own estate this week, and the CVE Watchlist on the site will keep doing that for you.

The year by month and severity

Every CVE published this year, placed by the month it appeared and the CVSS severity NVD assigned. Darker cells hold more CVEs; the number is the count. A pale right-hand column is normal in the current month, because NVD scores most CVEs a few days to weeks after publication.

	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP
CRITICAL	446	443	663	568	695	967	1,356	1,821	1,101
HIGH	1,621	1,623	2,586	2,228	2,839	3,358	4,174	5,268	4,679
MEDIUM	1,898	2,041	2,477	2,469	2,829	3,090	3,483	3,757	3,454
LOW	276	443	506	545	569	523	596	715	663
NOT YET SCORED	902	258	72	75	53	63	310	1,158	1,025
ALL	**5,143**	**4,808**	**6,304**	**5,885**	**6,985**	**8,001**	**9,919**	**12,719**	**10,922**

Counts by publication month and CVSS v3/v4 base severity. Not-yet-scored CVEs are shown separately rather than assumed low.

Severity against exploitability

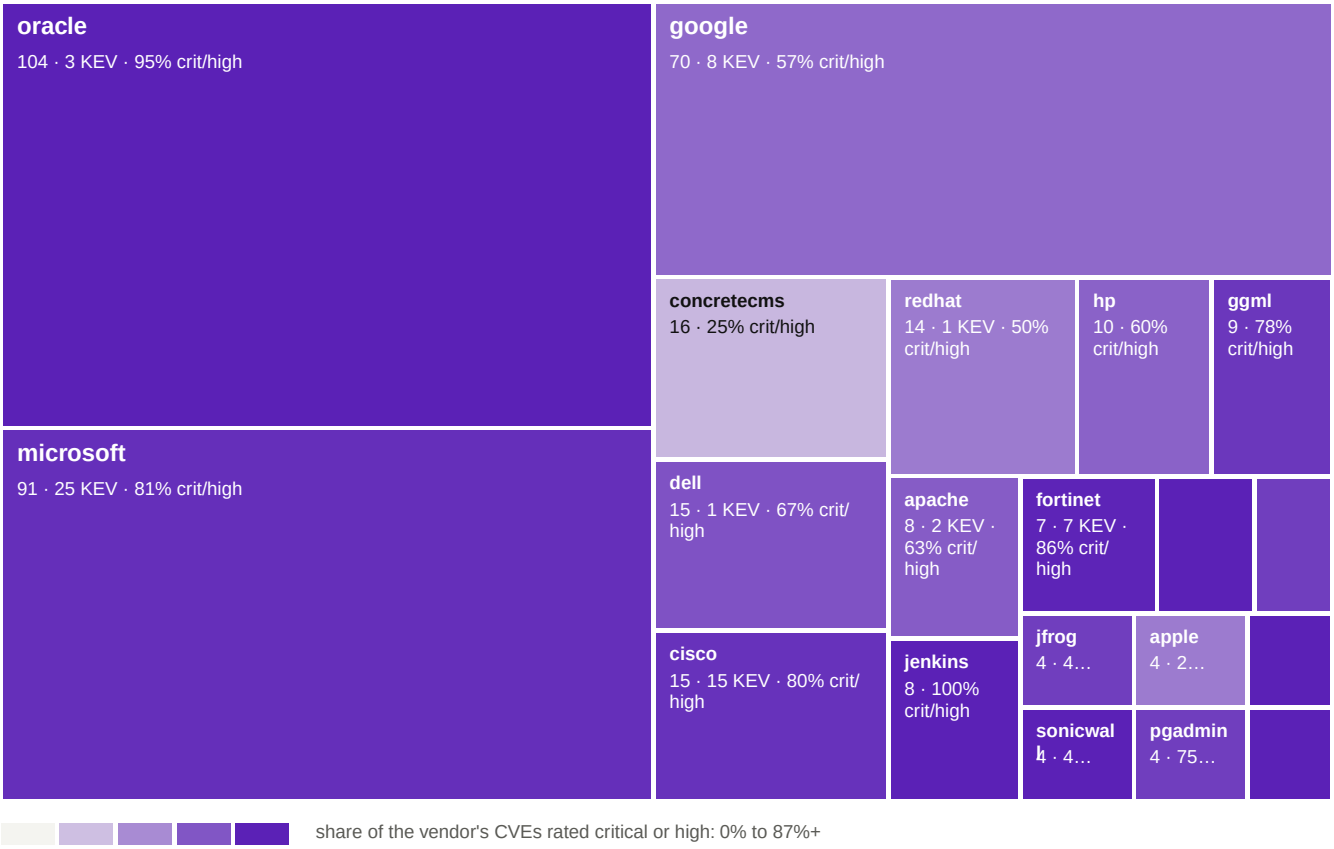
The same CVEs, placed by severity (rows) and by the strongest evidence of exploitation available for them (columns), most serious first: in CISA's Known Exploited Vulnerabilities catalogue, a public exploit in Exploit-DB, an EPSS probability of ten per cent or more, one to ten per cent, or below one per cent. Each CVE appears once, in the leftmost column it qualifies for. The percentage is the share of that severity row.

	IN CISA KEV	PUBLIC EXPLOIT	EPSS 10%+	EPSS 1–10%	EPSS < 1% OR UNSCORED
CRITICAL 8,060	**85** 1.1%	**36** 0.4%	**81** 1.0%	**696** 8.6%	**7,162** 88.9%
HIGH 28,376	**61** 0.2%	**46** 0.2%	**73** 0.3%	**1,219** 4.3%	**26,977** 95.1%
MEDIUM 25,498	**15** 0.1%	**20** 0.1%	**18** 0.1%	**260** 1.0%	**25,185** 98.8%
LOW 4,836	·	**3** 0.1%	**26** 0.5%	**255** 5.3%	**4,552** 94.1%
NOT YET SCORED 3,916	·	·	·	**1** 0.0%	**3,915** 100.0%

The top-left corner is where an emergency change is justified. Most of the year's critical CVEs sit in the right-hand columns: high impact if exploited, with no sign yet that anyone is exploiting them.

Which vendors carry the volume

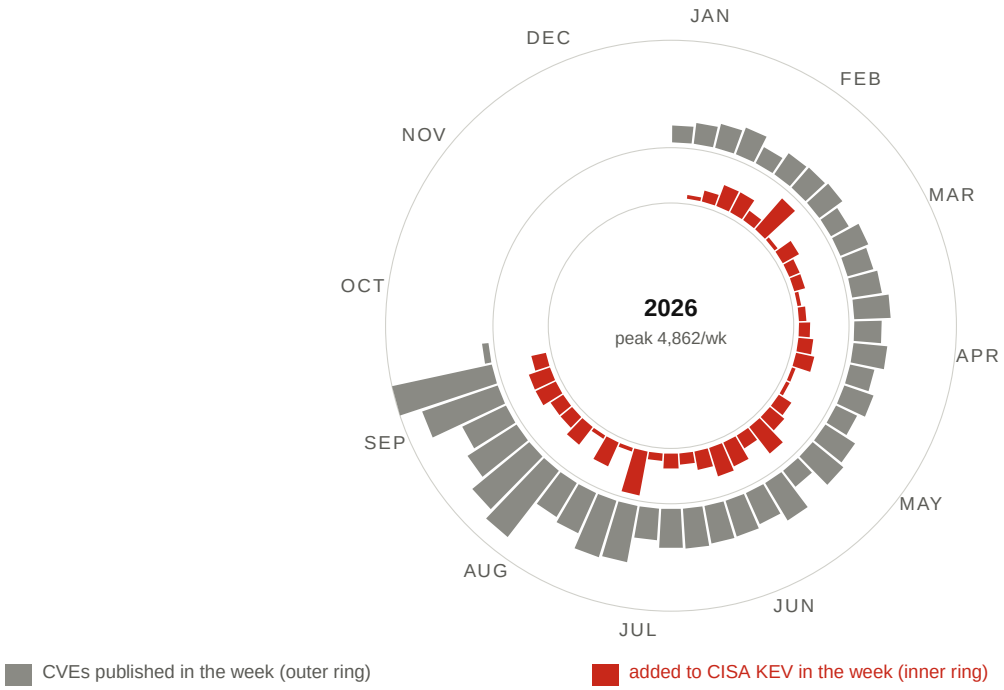
The 20 vendors with the most CVEs published this year, sized by count and shaded by the share of those CVEs rated critical or high. A large pale block is a vendor that publishes a great deal and scores most of it moderately; a small dark block is one whose few CVEs tend to be serious. KEV entries are noted where a vendor has any.



Vendor names as NVD's CPE data records them. A CVE that affects several vendors' products is counted once per vendor, so the blocks do not sum to the year's total.

The rhythm of the year

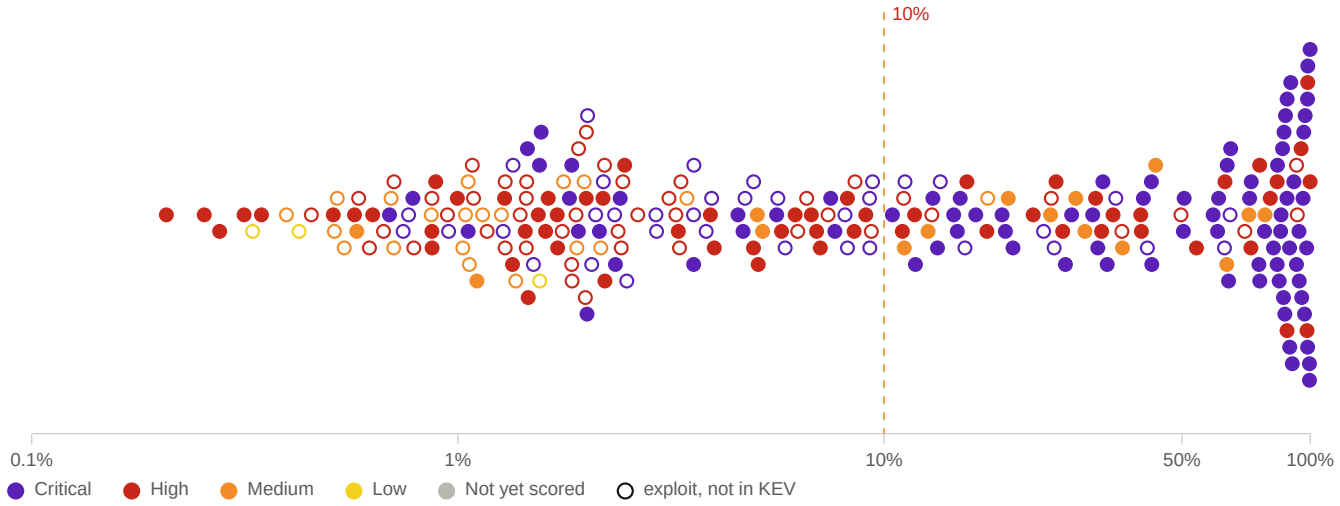
CVE publication by ISO week, drawn around the year. The outer grey bars are all CVEs published in the week; the inner red bars are the week's additions to CISA KEV. Patch Tuesdays and coordinated disclosure windows show up as spokes.



Weeks run clockwise from January at the top. Bar length is proportional to count; the two rings are scaled independently.

How the exploited minority scores

Every CVE published this year that is in CISA KEV or has a public exploit — 266 of them — placed along the EPSS axis (log scale) and coloured by severity. The dashed line is ten per cent. Points to the left of it are the case for not relying on EPSS alone: known exploitation with a low model score.



Each point is one CVE. Filled points are in CISA KEV; hollow points have a public exploit but are not in KEV. EPSS is FIRST's estimate of the probability of exploitation in the next thirty days.

Added to CISA KEV this year

Most recent first. Each is confirmed exploitation in the wild; the due date is CISA's remediation deadline for US federal agencies and a fair proxy for urgency everywhere else.

CVE	TITLE	SEVERITY	EPSS	ADDED	DUE
CVE-2026-7273	Zyxel GS1900 Series Switches Stack-Based Buffer Overflow Vulnerability	HIGH	0.32%	2026-09-21	2026-09-24
CVE-2025-39682	Linux Kernel Improper Check for Unusual or Exceptional Conditions Vulnerability	CRITICAL	1.20%	2026-09-18	2026-09-21
CVE-2025-39964	Linux Kernel Race Condition Vulnerability	MEDIUM	0.79%	2026-09-18	2026-09-21
CVE-2026-53266	Linux Kernel Out-of-Bounds Write Vulnerability	HIGH	0.28%	2026-09-18	2026-09-21
CVE-2026-58704	Google Pixel Improper Authorization Vulnerability	HIGH	0.21%	2026-09-16	2026-09-19
CVE-2026-76460	Cisco Identity Services Engine Incorrect Use of Privileged APIs Vulnerability	CRITICAL	0.78%	2026-09-16	2026-09-19
CVE-2026-87886	Acronis Backup Incorrect Default Permissions Vulnerability	HIGH	0.25%	2026-09-16	2026-09-19
CVE-2026-76461	Cisco Secure Email Gateway SQL Injection Vulnerability	CRITICAL	2.01%	2026-09-14	2026-09-17
CVE-2026-42016	JFrog Artifactory Incorrect Authorization Vulnerability	HIGH	9.06%	2026-09-11	2026-09-25
CVE-2026-42018	JFrog Artifactory Improper Authentication Vulnerability	HIGH	11.0%	2026-09-11	2026-09-25
CVE-2026-84869	ConnectWise ScreenConnect Improper Privilege Management and Missing Authorization Vulnerability	CRITICAL	0.69%	2026-09-11	2026-09-14
CVE-2026-85706	GitLab Community Edition and Enterprise Edition Path Traversal Vulnerability	CRITICAL	14.6%	2026-09-11	2026-09-14
CVE-2026-67277	MikroTik RouterOS Missing Authentication for Critical Function Vulnerability	HIGH	0.87%	2026-09-10	2026-09-13
CVE-2026-86060	MikroTik RouterOS Improper Neutralization of Argument Delimiters in a Command Vulnerability	CRITICAL	1.06%	2026-09-10	2026-09-13
CVE-2025-25249	Fortinet Multiple Products Heap-based Buffer Overflow Vulnerability	CRITICAL	2.40%	2026-09-09	2026-09-12
CVE-2026-19490	Citrix NetScaler Authentication Bypass Using an Alternate Path or Channel Vulnerability	CRITICAL	5.60%	2026-09-09	2026-09-12
CVE-2026-20079	Cisco Firewall Management Center Authentication Bypass Using an Alternate Path or Channel Vulnerability	CRITICAL	75.8%	2026-09-09	2026-09-12
CVE-2026-87491	Google Chromium V8 Out of Bounds Write Vulnerability	HIGH	1.00%	2026-09-09	2026-09-23
CVE-2026-75650	Adobe Commerce and Magento Improper Neutralization of Special Elements Used in a Template Engine Vulnerability	CRITICAL	2.15%	2026-09-08	2026-09-11
CVE-2026-81963	Microsoft Windows Link Following Vulnerability	HIGH	0.63%	2026-09-08	2026-09-22
CVE-2026-85880	Microsoft Windows Heap-Based Buffer Overflow Vulnerability	HIGH	0.57%	2026-09-08	2026-09-22
CVE-2026-86218	N-able N-central Static Code Injection Vulnerability	CRITICAL	7.49%	2026-09-08	2026-09-11
CVE-2026-85046	Google Chromium V8 Type Confusion Vulnerability	HIGH	1.46%	2026-09-04	2026-09-18
CVE-2026-48710	Kludex Starlette HTTP Request/Response Smuggling Vulnerability	MEDIUM	36.3%	2026-09-02	2026-09-16
CVE-2026-49869	Kestra OSS OS Command Injection Vulnerability	CRITICAL	1.92%	2026-09-02	2026-09-05

Gained a public exploit this year

CVEs whose first Exploit-DB entry was published this year, most recent first. A public exploit removes the skill barrier; these appear in scanning traffic within days.

CVE	TITLE	SEVERITY	EPSS	EXPLOITS	FIRST
CVE-2026-80428	ILIAS before versions 9.22, 10.10, and 11.3 contains an unauthenticated PHP object injection vulnerability that allows unauthenticated attackers to execute arbitrary code by injecting serialized objects through the LTI authentication endpoint and…	CRITICAL	2.33%	1	2026-09-11
CVE-2025-57819	Sangoma FreePBX Authentication Bypass Vulnerability	CRITICAL	85.5%	1	2026-09-03

CVE	TITLE	SEVERITY	EPSS	EXPLOITS	FIRST
CVE-2026-59827	Prior to 1.58.15, 1.59.12, 1.60.6.3, and 1.61.1.4, Metabase instances with an H2 database connection, including the default sample database, deserialize arbitrary Java objects returned in H2 native query result columns of type OTHER without validation,…	HIGH	3.25%	1	2026-09-03
CVE-2026-39987	Marimo Remote Code Execution Vulnerability	CRITICAL	99.6%	1	2026-09-02
CVE-2026-9198	IBM Langflow Code Injection Vulnerability	CRITICAL	60.6%	1	2026-09-02
CVE-2026-29053	From version 0.7.2 to 6.19.0, specifically crafted malicious themes can execute arbitrary code on the server running Ghost.	CRITICAL	3.58%	1	2026-09-02
CVE-2026-41456	Bludit CMS prior to commit 6732dde contains a reflected cross-site scripting vulnerability in the search plugin that allows unauthenticated attackers to inject arbitrary JavaScript by crafting a malicious search query.	MEDIUM	1.90%	1	2026-09-02
CVE-2025-68137	Prior to version 2025.10.0, an integer overflow occurring in `SdpPacket::parse_header()` allows the current buffer length to be set to 7 after a complete header of size 8 has been read.	HIGH	1.09%	1	2026-09-02
CVE-2025-70336	A Stored cross-site scripting (XSS) vulnerability in 'Create New Live Item' in PodcastGenerator 3.2.9 allows remote attackers to inject arbitrary script or HTML via the 'TITLE', 'SHORT DESCRIPTION' and 'LONG DESCRIPTION' parameters.	MEDIUM	0.40%	1	2026-09-02
CVE-2026-65008	Grav 2.0.4 (fixed in 2.0.7) contains a remote code execution vulnerability in Blueprint::dynamicData() (system/src/Grav/Common/Data/Blueprint.php), which passes a Class::method callable string and its arguments directly to call_user_func_array() without…	CRITICAL	2.02%	1	2026-09-01
CVE-2026-15013	The SAML Single Sign On – SSO Login plugin for WordPress is vulnerable to Authentication Bypass via SAML Signature Algorithm Confusion in all versions up to, and including, 5.4.3.	CRITICAL	1.50%	1	2026-09-01
CVE-2026-67206	Wolf CMS through 0.8.3.1 contains a remote code execution vulnerability in FileManagerController that allows authenticated attackers to create arbitrary PHP files by exploiting missing file extension validation in the create_file() and save() functions.	HIGH	1.40%	1	2026-09-01
CVE-2025-50455	SQL injection vulnerability exists in the order_by parameter of the /customers/search endpoint in Alex Tselegidis EasyAppointments <= 1.5.1.	CRITICAL	0.95%	1	2026-09-01
CVE-2026-25544	Prior to 3.73.0, when querying JSON or richText fields, user input was directly embedded into SQL without escaping, enabling blind SQL injection attacks.	CRITICAL	0.77%	1	2026-09-01
CVE-2026-5027	The 'POST /api/v2/files' endpoint does not sanitize the 'filename' parameter from the multipart form data, allowing an attacker to write files to arbitrary locations on the filesystem using path traversal sequences ('../').	HIGH	36.1%	1	2026-08-31
CVE-2025-60689	An unauthenticated command injection vulnerability exists in the Start_EPI function of the httpd binary on Linksys E1200 v2 routers (Firmware E1200_v2.0.11.001_us.tar.gz).	MEDIUM	17.5%	1	2026-08-31
CVE-2026-51134	The C-MOR Video Surveillance web interface (up to version 6.0104) is vulnerable to Path Traversal via the 'cam' parameter in show-movies.pml.	HIGH	1.89%	1	2026-08-31
CVE-2026-54647	An authenticated administrator can supply a comma-delimited value that changes the SET clause because HTML sanitization does not neutralize SQL syntax, allowing manipulation of database columns and potentially other data within the application's…	HIGH	1.45%	1	2026-08-31
CVE-2026-54646	An authenticated administrator can terminate the quoted identifier with a closing backtick and introduce attacker-controlled structural SQL, potentially compromising database confidentiality, integrity, and availability within the application's database…	HIGH	1.45%	1	2026-08-31
CVE-2026-54645	An administrator with product-editing rights can store event-handler attributes, SVG content, or javascript: URIs that bypass this filter, causing persistent JavaScript execution when a storefront visitor or another administrator views the product…	MEDIUM	1.26%	1	2026-08-31

Highest EPSS among this year's CVEs

The fifteen CVEs published this year that FIRST currently rates most likely to be exploited in the next thirty days.

CVE	TITLE	SEVERITY	EPSS	KEV	PUBLISHED
CVE-2026-10520	Ivanti Sentry OS Command Injection Vulnerability	CRITICAL	99.9%	yes	2026-06-09
CVE-2026-31431	Linux Kernel Incorrect Resource Transfer Between Spheres Vulnerability	HIGH	99.9%	yes	2026-04-22
CVE-2026-8037	Progress LoadMaster Command Injection Vulnerability	CRITICAL	99.6%	yes	2026-06-04
CVE-2026-39987	Marimo Remote Code Execution Vulnerability	CRITICAL	99.6%	yes	2026-04-09
CVE-2026-1340	Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability	CRITICAL	98.7%	yes	2026-01-29
CVE-2026-34486	Apache Tomcat Missing Encryption of Sensitive Data Vulnerability	HIGH	98.6%	yes	2026-04-09
CVE-2026-1281	Ivanti Endpoint Manager Mobile (EPMM) Code Injection Vulnerability	CRITICAL	98.6%	yes	2026-01-29
CVE-2026-41940	WebPros cPanel & WHM and WP2 (WordPress Squared) Missing Authentication for Critical Function Vulnerability	CRITICAL	98.5%	yes	2026-04-29
CVE-2026-34197	Apache ActiveMQ Improper Input Validation Vulnerability	HIGH	98.3%	yes	2026-04-07
CVE-2026-24061	GNU InetUtils Argument Injection Vulnerability	CRITICAL	98.1%	yes	2026-01-21
CVE-2026-63030	WordPress Core Interpretation Conflict Vulnerability	CRITICAL	97.3%	yes	2026-07-17
CVE-2026-20253	Splunk Enterprise Missing Authentication for Critical Function Vulnerability	CRITICAL	96.9%	yes	2026-06-10
CVE-2026-23760	SmarterTools SmarterMail Authentication Bypass Using an Alternate Path or Channel Vulnerability	CRITICAL	96.5%	yes	2026-01-22
CVE-2026-33017	Langflow Code Injection Vulnerability	CRITICAL	96.2%	yes	2026-03-20
CVE-2026-35273	Oracle PeopleSoft Enterprise PeopleTools Missing Authentication for Critical Function Vulnerability	CRITICAL	95.5%	yes	2026-06-11

What to do with this

Start with the KEV additions and anything with a public exploit that is in your estate: those are emergency changes, and an overdue KEV entry is also a reason to look for prior compromise. Then take the EPSS-ten-per-cent group into the next change window. Everything else goes through the normal cycle in CVSS order, which for most organisations is the calm majority of the year.

The same data is free on the site. The CVE Explorer (cyber-defence.io/tools/cve) carries every record with a plain-English verdict and a JSON export; the CVE Watchlist narrows all of this to the products you actually run and will email you when something changes; the KEV calendar shows the deadlines as a calendar you can subscribe to. If you would rather someone did the checking for you, that is what our managed SOC does every day for clients: the same feeds, matched against their estate, with an analyst on the other end.

UK CYBER DEFENCE LTD · HELLO@CYBER-DEFENCE.IO · HTTPS://WWW.CYBER-DEFENCE.IO/TOOLS/CVE

Sources: NVD (National Vulnerability Database), FIRST EPSS, CISA Known Exploited Vulnerabilities catalogue, Exploit-DB. Counts reflect the data as held by the CVE Explorer at the generation time above; NVD scores lag publication, so recent months under-count severity.