2025 Vulnerability Report: Observations and Weighted Analysis

Vulnerability trends, exploitation sightings, and vendor/weakness patterns

CIRCL - Computer Incident Response Center Luxembourg

2026-05-11

CIRCL
Computer Incident
Response Center
Luxembourg

Contents

{{< card link="/tags/vulnerabilityreport/" title="All vulnerability reports" icon="document-report" >}}

{{< callout type="info" >}} This report was generated with the help of AI, leveraging the VulnMCP Model Context Protocol server connected to Vulnerability-Lookup. The underlying data was aggregated from the twelve monthly reports published throughout 2025 and from the live Vulnerability-Lookup API. {{< /callout >}}

0.1 Introduction

The 2025 threat landscape was characterised by sustained pressure on enterprise infrastructure, edge devices, and developer tooling. Attackers continued to weaponise newly disclosed vulnerabilities within hours of publication, while a long tail of unpatched **legacy IoT and edge devices** (D-Link, Zyxel, DASAN, Huawei, Realtek, Netgear) kept generating massive exploitation noise. Several flagship incidents shaped the year: the **SAP NetWeaver Visual Composer** zero-day exploitation in April, the **SharePoint "ToolShell"** campaign in July, the **NetScaler "CitrixBleed 2"** saga from June onward, the **Oracle E-Business Suite** exploitation tied to the Cl0p activity in October, the **WSUS critical** (CVE-2025-59287) in October-November, the **FortiWeb** authentication bypasses in November, and the dramatic **React Server Components ("React2Shell")** surge in December.

This year-in-review consolidates the twelve monthly reports covering 2025 and aggregates the data collected by Vulnerability-Lookup. Sources used to build this report include:

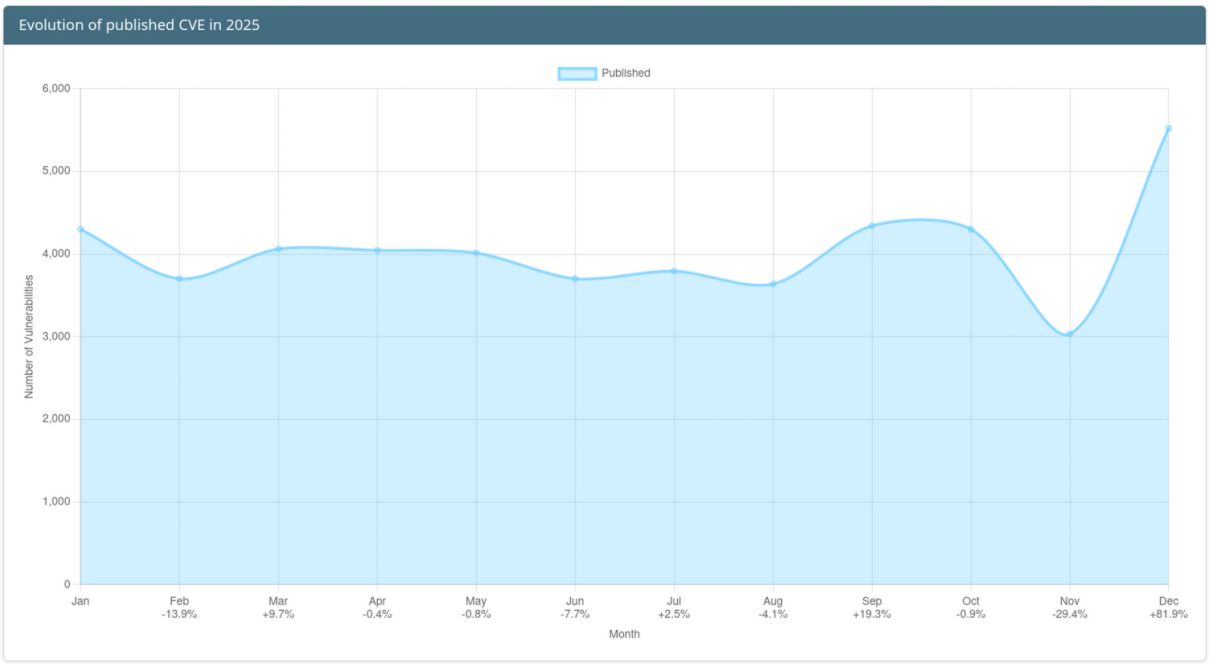
- **Vulnerability-Lookup** sightings
- **CISA KEV** catalog
- **CIRCL** team curation and security advisories
- **EUVD / ENISA** Known Exploited Vulnerabilities catalog
- Community contributors via comments and bundles on the platform
- Sighting feeds: MISP, Exploit-DB, Bluesky, Mastodon, GitHub Gists, The Shadowserver Foundation honeypots, Nuclei, SPLOITUS, Metasploit, Telegram, and more.

This report was generated with AI assistance via **VulnMCP**, the Model Context Protocol server that exposes Vulnerability-Lookup capabilities to AI agents: **https://github.com/vulnerability-lookup/VulnMCP**.

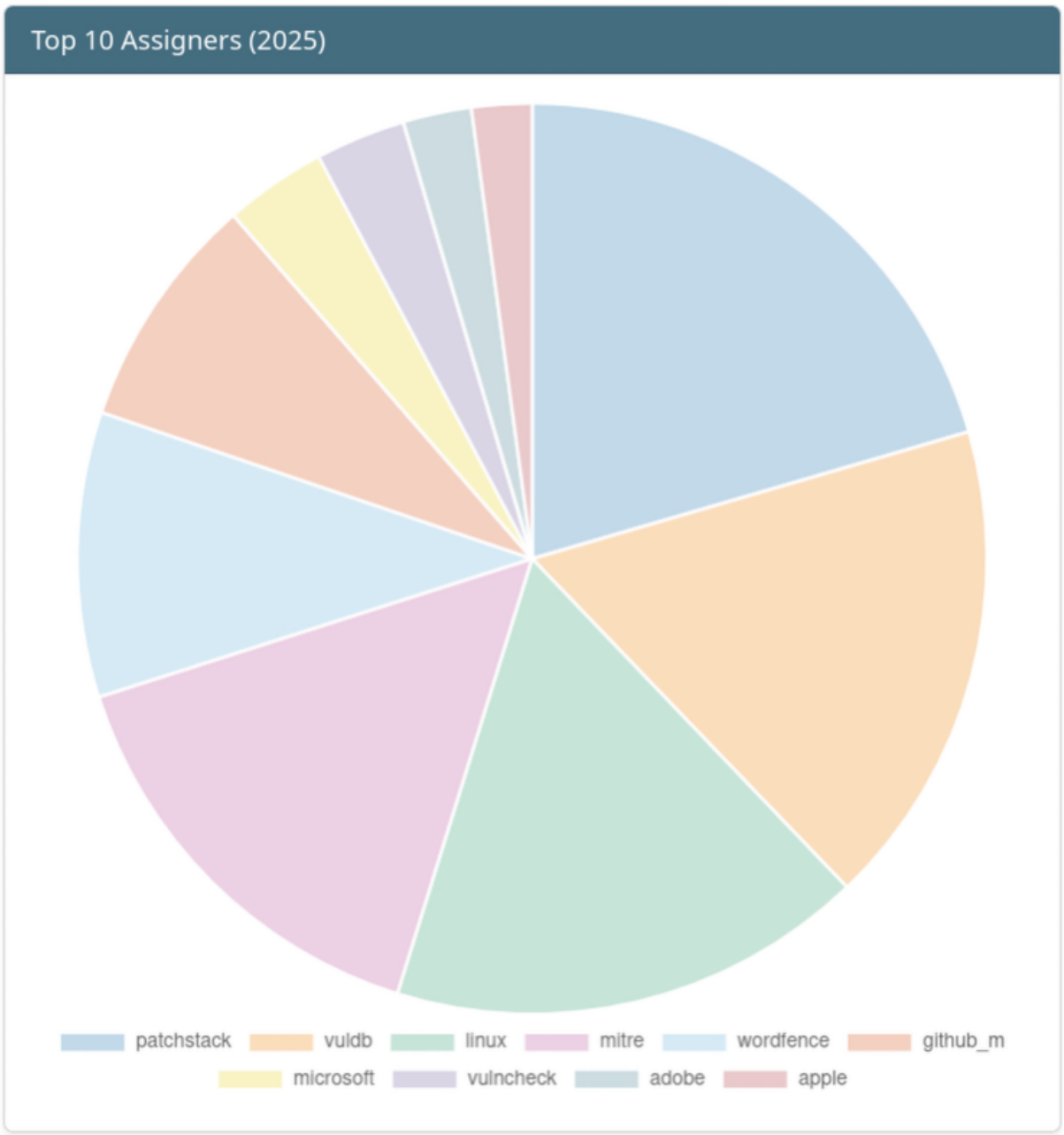
0.2 The Year at a Glance

The charts below summarise publication trends and the ecosystem most affected throughout 2025.

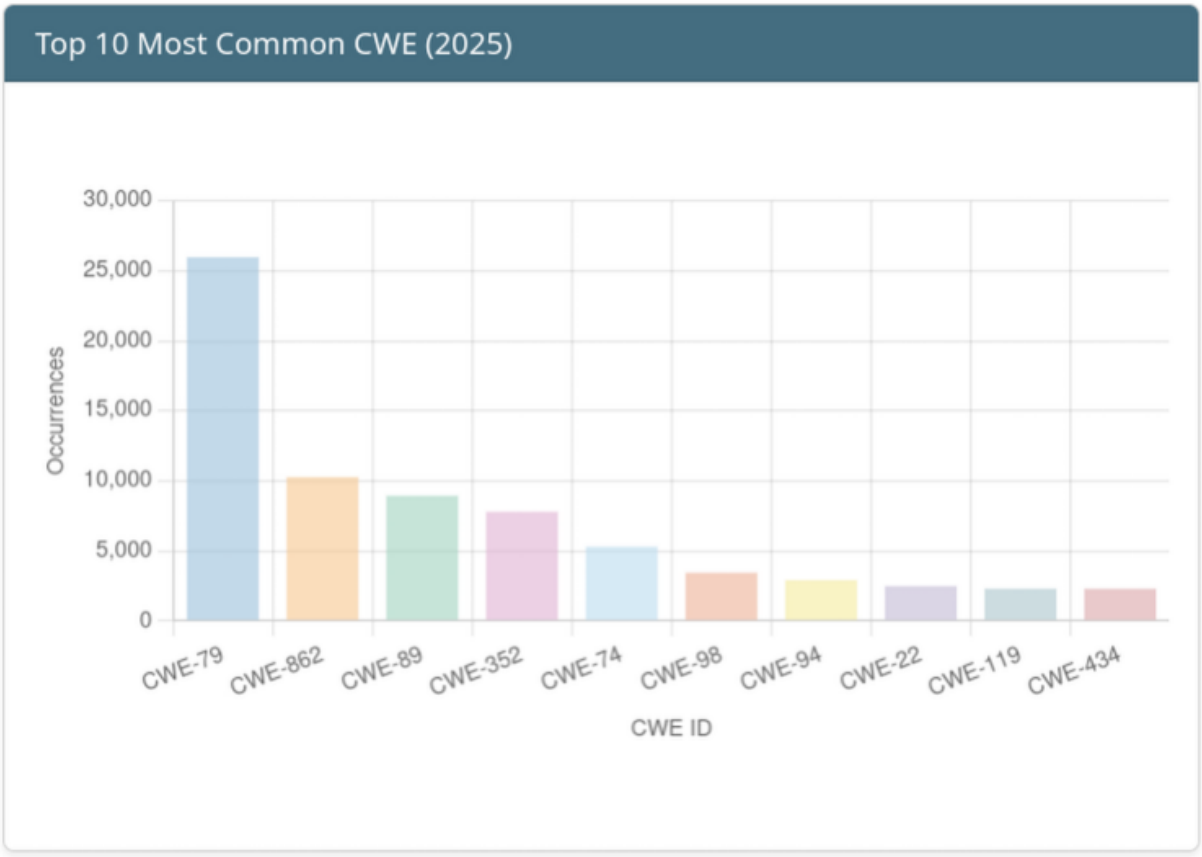
0.2.1 Evolution of CVE publication



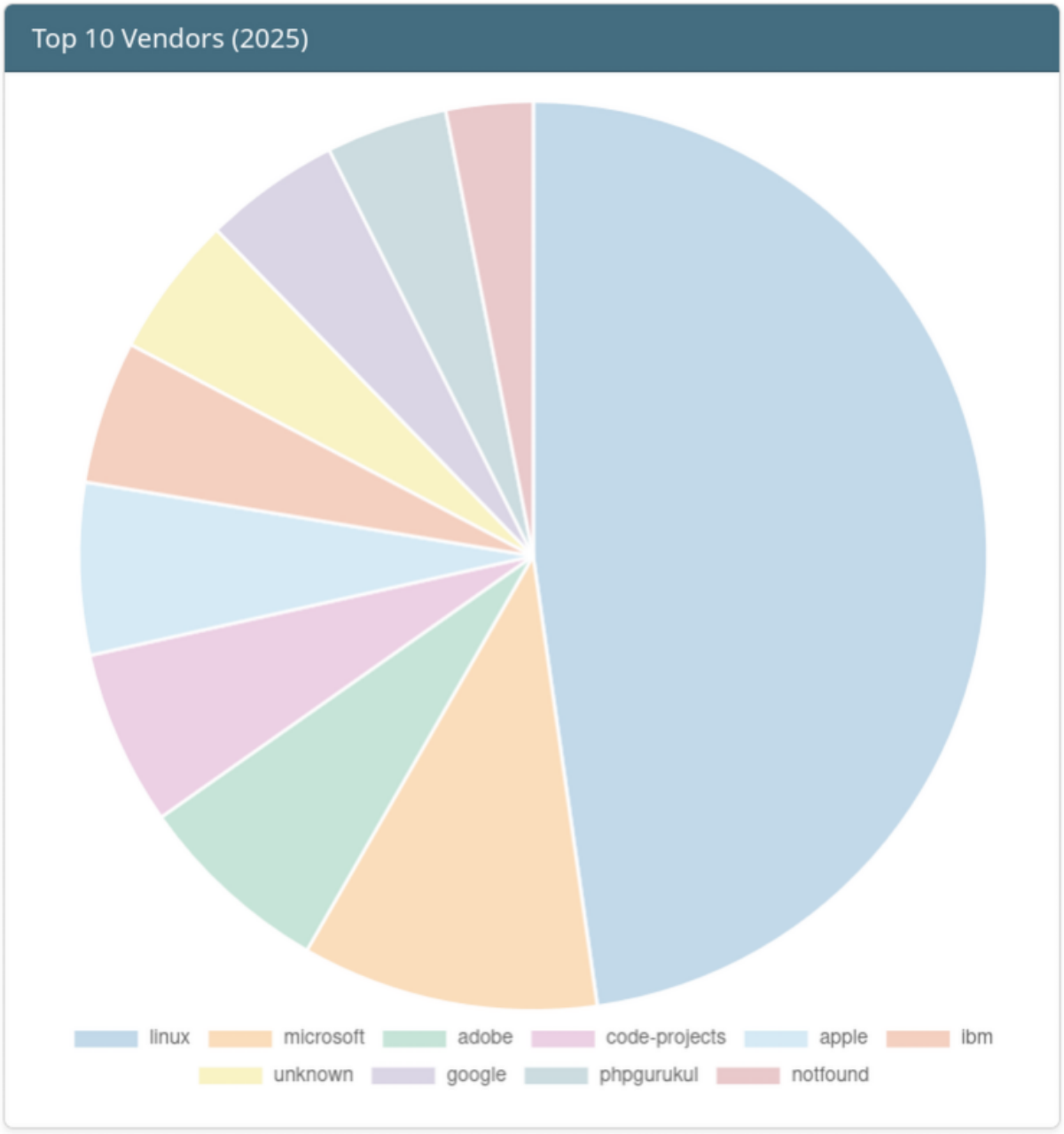
0.2.2 Top 10 CVE Assigners of the Year



0.2.3 Top 10 Weaknesses (CWE) of the Year



0.2.4 Top 10 Vendors in 2025



0.2.5 Recurring themes

2025 delivered an unusually high volume of *actively exploited* vulnerabilities. Recurring themes across the year include:

- **Edge & network devices** dominated continuous exploitation: D-Link DIR-645 (CVE-2015-2051),

Zyxel P660HN (CVE-2017-18368), DASAN GPON (CVE-2018-10562), Huawei HG532 (CVE-2017-17215) remained in the top sightings *every single month*.

- **VPN / remote access**: Ivanti Connect Secure (CVE-2025-0282, CVE-2025-22457), NetScaler ADC (CVE-2025-5777, CVE-2025-6543), Fortinet FortiOS / FortiWeb / FortiSwitchManager, Palo Alto PAN-OS (CVE-2025-0108), SonicWall SMA, Check Point Quantum.
- **Enterprise platforms**: SAP NetWeaver (CVE-2025-31324), Microsoft SharePoint (CVE-2025-53770), Microsoft Exchange (CVE-2025-53786), Microsoft WSUS (CVE-2025-59287), Oracle E-Business Suite (CVE-2025-61882), Oracle Identity Manager (CVE-2025-61757).
- **Developer ecosystem & supply chain**: Next.js middleware bypass (CVE-2025-29927), Apache Tomcat (CVE-2025-24813), Erlang/OTP SSH (CVE-2025-32433), `tj-actions/changed-files` GitHub Action compromise (CVE-2025-30066), React Server Components "React2Shell" (CVE-2025-55182), npm `qix/duckdb_admin` account compromise.
- **Client-side**: Apple iOS/iPadOS/visionOS, Google Chrome V8, WinRAR (CVE-2025-8088, CVE-2025-6218), 7-Zip (CVE-2025-11001), Samsung Mobile zero-days (CVE-2025-21042, CVE-2025-21043).
- **CWE landscape**: Cross-site scripting (CWE-79) and SQL injection (CWE-89) consistently topped the weakness charts, followed by injection (CWE-74), code injection (CWE-94), and memory safety issues (CWE-119/121/122/125/416).

In total, our community recorded **tens of thousands of sightings** in 2025, with hundreds of patches released, dozens of public proofs of concept, and numerous in-the-wild exploitations confirmed by The Shadowserver Foundation honeypot network, CISA KEV additions, and contributor reports.

0.3 Top 50 Vulnerabilities of the Year

Most-sighted vulnerabilities recorded by Vulnerability-Lookup between **2025-01-01** and **2025-12-31**. Severities are derived from the VLAI classifier.

Vulnerability	Sighting Count	Vendor	Product	VLAI Severity
CVE-2025-55182	1138	Meta	react-server-dom-webpack	Critical
CVE-2015-2051	726	D-Link	DIR-645	High
CVE-2017-18368	710	ZyXEL	P660HN-T1A	Critical
CVE-2025-5777	671	NetScaler	ADC	Critical
CVE-2018-10562	627	DASAN Networks	GPON Router	Critical

Vulnerability	Sighting Count	Vendor	Product	VLAI Severity
CVE-2025-53770	619	Microsoft	SharePoint Enterprise Server 2016	Critical
CVE-2025-31324	566	SAP	SAP NetWeaver (Visual Composer)	Critical
CVE-2018-14774	542	Symfony	HttpKernel	Medium
CVE-2025-0108	524	Palo Alto Networks	PAN-OS / Cloud NGFW	High
CVE-2021-44228	493	Apache Software Foundation	Apache Log4j2	Critical
CVE-2023-20198	472	Cisco	Cisco IOS XE Software	High
CVE-2017-17215	462	Huawei	HG532	Critical
CVE-2017-9841	444	PHPUnit	PHPUnit	Critical
CVE-2016-1555	437	Netgear	WNAP320	Critical
CVE-2014-8361	435	Realtek	Realtek SDK	Critical
CVE-2023-22527	434	Atlassian	Confluence Data Center	Critical
CVE-2019-12780	429	Belkin	Wemo Crock-Pot	High
CVE-2025-29927	427	Vercel	Next.js	Critical
CVE-2024-3721	426	TBK	DVR-4104 / DVR-4216	Medium
CVE-2016-6277	424	Netgear	D6220 / R-series	High
CVE-2025-59287	418	Microsoft	Windows Server (WSUS)	Critical
CVE-2016-10372	418	eir	D1000 modem	Critical
CVE-2019-1653	408	Cisco	Small Business RV320/RV325	High
CVE-2021-26855	401	Microsoft	Exchange Server (ProxyLogon)	Critical

Vulnerability	Sighting Count	Vendor	Product	VLAI Severity
CVE-2021-42013	391	Apache Software Foundation	Apache HTTP Server	Critical
CVE-2023-0656	380	SonicWall	SonicOS	High
CVE-2023-42793	377	JetBrains	TeamCity	Critical
CVE-2018-13379	375	Fortinet	FortiOS / FortiProxy	Critical
CVE-2025-0282	369	Ivanti	Connect Secure	Critical
CVE-2022-26134	366	Atlassian	Confluence Data Center	Critical
CVE-2023-38646	366	Metabase	Metabase	Critical
CVE-2020-25506	360	D-Link	DNS-320 NAS	High
CVE-2018-7600	355	Drupal	Drupal Core (Drupalgeddon 2)	Critical
CVE-2024-28995	348	SolarWinds	Serv-U	High
CVE-2023-23752	343	Joomla!	Joomla! CMS	High
CVE-2024-36401	341	OSGeo	GeoServer / GeoTools	Critical
CVE-2022-22274	335	SonicWall	SonicOS	High
CVE-2024-4577	333	PHP Group	PHP	Critical
CVE-2020-8191	328	Citrix	ADC / Gateway	Medium
CVE-2025-61882	327	Oracle Corporation	Oracle Concurrent Processing (EBS)	Critical
CVE-2011-3600	322	Apache	OFBiz	High
CVE-2021-32030	320	ASUS	GT-AC2900 / Lyra Mini Routers	High
CVE-2023-26801	318	LB-LINK	BL-AC1900 / BL-WR9000 routers	High

Vulnerability	Sighting Count	Vendor	Product	VLAI Severity
CVE-2019-17506	312	D-Link	DIR-868L / DIR-817LW	High
CVE-2025-24813	307	Apache Software Foundation	Apache Tomcat	Critical
CVE-2025-8088	307	win.rar GmbH	WinRAR	High
CVE-2024-24919	299	Check Point	Quantum Security Gateways	High
CVE-2016-10108	290	Western Digital	MyCloud NAS	High
CVE-2021-3129	284	Laravel	Ignition	Critical
CVE-2025-32433	282	Erlang	OTP (SSH)	Critical

0.3.1 Top 10 Vulnerabilities per Month

Aggregated from the published monthly reports. The metrics differ slightly across months (some months use sighting counts, others a curated Top ranking).

0.3.1.1 January 2025 Top vulnerabilities sourced from the January 2025 report:

Vulnerability	Vendor	Product	Severity
CVE-2025-0282	Ivanti	Connect Secure	9.0 (Critical)
CVE-2024-55591	Fortinet	FortiOS	9.8 (Critical)
CVE-2024-49113	Microsoft	Windows 10 (LDAP)	7.5 (High)
CVE-2015-2051	D-Link	DIR-645	8.8 (High)
CVE-2025-24085	Apple	visionOS / iOS	7.3 (High)
CVE-2025-0283	Ivanti	Connect Secure	7.0 (High)
CVE-2018-10562	DASAN Networks	GPON Router	9.8 (Critical)
CVE-2017-17215	Huawei	HG532	8.8 (High)
CVE-2024-7344	Radix	SmartRecovery	8.2 (High)
CVE-2024-50603	Aviatrix	Controller	10.0 (Critical)

0.3.1.2 February 2025

Top vulnerabilities sourced from the February 2025 report:

Vulnerability	Vendor	Product	Severity
CVE-2025-0282	Ivanti	Connect Secure	9.0 (Critical)
CVE-2024-55591	Fortinet	FortiOS	9.8 (Critical)
CVE-2024-49113	Microsoft	Windows 10 (LDAP)	7.5 (High)
CVE-2015-2051	D-Link	DIR-645	9.8 (Critical)
CVE-2017-18368	ZyXEL	P660HN-T1A	9.8 (Critical)
CVE-2025-0283	Ivanti	Connect Secure	7.0 (High)
CVE-2024-7344	Radix	SmartRecovery	8.2 (High)
CVE-2017-17215	Huawei	HG532	8.8 (High)
CVE-2018-10562	DASAN Networks	GPON Router	9.8 (Critical)
CVE-2024-50603	Aviatrix	Controller	10.0 (Critical)

0.3.1.3 March 2025

Top vulnerabilities sourced from the March 2025 report:

Vulnerability	Vendor	Product	Sightings	Severity
CVE-2025-29927	Vercel	Next.js	167	9.1 (Critical)
CVE-2025-24813	Apache Software Foundation	Apache Tomcat	128	9.2 (Critical)
CVE-2025-1974	Kubernetes	ingress-nginx	86	9.8 (Critical)
CVE-2024-4577	PHP Group	PHP	83	9.8 (Critical)
CVE-2025-22224	VMware	ESXi	80	9.3 (Critical)
CVE-2025-24201	Apple	iOS / iPadOS	79	7.0 (High)
CVE-2025-2783	Google	Chrome	72	8.3 (High)
CVE-2025-30066	tj-actions	changed-files	67	8.6 (High)
CVE-2017-18368	ZyXEL	P660HN-T1A	60	9.8 (Critical)
CVE-2015-2051	D-Link	DIR-645	60	8.8 (High)

0.3.1.4 April 2025

Top vulnerabilities sourced from the April 2025 report:

Vulnerability	Vendor	Product	Sightings	Severity
CVE-2025-22457	Ivanti	Connect Secure	188	9.0 (Critical)
CVE-2025-32433	Erlang	OTP (SSH)	119	10 (Critical)
CVE-2025-31161	CrushFTP	CrushFTP	108	9.8 (Critical)
CVE-2025-31324	SAP	NetWeaver Visual Composer	101	10 (Critical)
CVE-2025-29824	Microsoft	Windows (CLFS)	85	7.8 (High)
CVE-2025-24054	Microsoft	Windows (NTLM)	79	6.5 (Medium)
CVE-2025-30406	Gladinet	CentreStack	64	9.0 (Critical)
CVE-2025-24200	Apple	iPadOS	61	6.1 (Medium)
CVE-2017-18368	ZyXEL	P660HN-T1A	60	9.8 (Critical)
CVE-2015-2051	D-Link	DIR-645	60	8.8 (High)

0.3.1.5 May 2025 Top vulnerabilities sourced from the May 2025 report:

Vulnerability	Vendor	Product	VLAI Severity
CVE-2025-31324	SAP	NetWeaver Visual Composer	Critical
CVE-2025-4427	Ivanti	Endpoint Manager Mobile	Critical
CVE-2025-37899	Linux	Linux kernel (ksmbd)	High
CVE-2025-4428	Ivanti	Endpoint Manager Mobile	High
CVE-2025-32756	Fortinet	FortiVoice	Critical
CVE-2025-4664	Google	Chrome	Medium
CVE-2025-20188	Cisco	IOS XE Software	Critical
CVE-2017-18368	ZyXEL	P660HN-T1A	Critical
CVE-2015-2051	D-Link	DIR-645	Critical

Vulnerability	Vendor	Product	VLAI Severity
CVE-2024-38475	Apache Software Foundation	HTTP Server	Critical

0.3.1.6 June 2025

Top vulnerabilities sourced from the June 2025 report:

Vulnerability	Vendor	Product	VLAI Severity
CVE-2025-33053	Microsoft	Windows (WebDAV)	High
CVE-2025-49113	Roundcube	Webmail	High
CVE-2025-5777	NetScaler	ADC (“CitrixBleed 2”)	Critical
CVE-2025-5419	Google	Chrome	High
CVE-2025-2783	Google	Chrome	High
CVE-2025-6019	Red Hat	Red Hat Enterprise Linux	Medium
CVE-2025-33073	Microsoft	Windows SMB	High
CVE-2025-6543	NetScaler	ADC	Critical
CVE-2015-2051	D-Link	DIR-645	Critical
CVE-2017-18368	ZyXEL	P660HN-T1A	Critical

0.3.1.7 July 2025

Top vulnerabilities sourced from the July 2025 report:

Vulnerability	Vendor	Product	Sightings	VLAI Severity
CVE-2025-53770	Microsoft	SharePoint (“ToolShell”)	416	Critical
CVE-2025-5777	NetScaler	ADC	267	Critical
CVE-2025-25257	Fortinet	FortiWeb	145	Critical
CVE-2025-6554	Google	Chrome	130	High
CVE-2025-47812	wftpserver	Wing FTP Server	129	Critical

Vulnerability	Vendor	Product	Sightings	VLAI Severity
GHSA-269G-PWP5-87PP	junit-team	JUnit4	120	Medium
CVE-2025-53771	Microsoft	SharePoint	104	Medium
CVE-2025-49706	Microsoft	SharePoint	96	Medium
GHSA-78WR-2P64-HPWJ	Apache Software Foundation	Apache Commons IO	85	Medium
GHSA-5MG8-W23W-74H3	Google LLC	Guava	84	Low

0.3.1.8 August 2025

Top vulnerabilities sourced from the August 2025 report:

Vulnerability	Vendor	Product	Sightings	VLAI Severity
CVE-2025-8088	win.rar GmbH	WinRAR	193	High
CVE-2025-53786	Microsoft	Exchange Server	175	High
CVE-2025-43300	Apple	macOS / iOS	128	Medium
CVE-2025-6543	NetScaler	ADC	111	Critical
CVE-2025-25256	Fortinet	FortiSIEM	79	Critical
CVE-2025-9074	Docker	Docker Desktop	65	Critical
CVE-2015-2051	D-Link	DIR-645	62	Critical
CVE-2017-18368	ZyXEL	P660HN-T1A	61	Critical
CVE-2025-31324	SAP	NetWeaver Visual Composer	59	Critical
CVE-2025-5777	NetScaler	ADC	52	Critical

0.3.1.9 September 2025

Top vulnerabilities sourced from the September 2025 report:

Vulnerability	Vendor	Product	Sightings	VLAI Severity
CVE-2025-10585	Google	Chrome	94	High

Vulnerability	Vendor	Product	Sightings	VLAI Severity
CVE-2025-10035	Fortra	GoAnywhere MFT	79	Critical
CVE-2025-42957	SAP	S/4HANA	71	Critical
CVE-2025-55241	Microsoft	Entra	68	High
CVE-2025-54236	Adobe	Commerce	64	Critical
CVE-2024-50264	Linux	Linux kernel	60	High
CVE-2015-2051	D-Link	DIR-645	58	High
CVE-2023-51767	OpenSSH	OpenSSH	57	High
CVE-2017-18368	ZyXEL	P660HN-T1A	57	Critical
CVE-2025-43300	Apple	iOS / iPadOS	54	High

0.3.1.10 October 2025 Top vulnerabilities sourced from the October 2025 report:

Vulnerability	Vendor	Product	Sightings	VLAI Severity
CVE-2025-61882	Oracle Corporation	Oracle Concurrent Processing (EBS)	241	Critical
CVE-2025-59287	Microsoft	Windows Server (WSUS)	235	Critical
CVE-2025-49844	Redis	Redis	106	Critical
CVE-2025-59489	Unity3D	Unity Editor	98	High
CVE-2025-61884	Oracle Corporation	Oracle Configurator	95	High
CVE-2025-54236	Adobe	Commerce	94	Critical
CVE-2025-55315	Microsoft	ASP.NET Core 8.0	75	High
CVE-2015-2051	D-Link	DIR-645	64	High
CVE-2025-20352	Cisco	IOS	63	High
CVE-2017-18368	ZyXEL	P660HN-T1A	63	Critical

0.3.1.11 November 2025

Top vulnerabilities sourced from the November 2025 report:

Vulnerability	Vendor	Product	Sightings	VLAI Severity
CVE-2025-64446	Fortinet	FortiWeb	105	Critical
CVE-2025-59287	Microsoft	Windows Server (WSUS)	88	Critical
CVE-2025-21042	Samsung Mobile	Samsung Mobile Devices	86	High
CVE-2025-58034	Fortinet	FortiWeb	84	High
CVE-2025-13223	Google	Chrome	84	High
CVE-2023-20198	Cisco	IOS XE Software	71	High
CVE-2025-61757	Oracle Corporation	Identity Manager	67	Critical
CVE-2025-11001	7-Zip	7-Zip	65	High
CVE-2025-12480	TrioFox	TrioFox	64	Critical
CVE-2015-2051	D-Link	DIR-645	59	High

0.3.1.12 December 2025

Top vulnerabilities sourced from the December 2025 report:

Vulnerability	Vendor	Product	Sightings	VLAI Severity
CVE-2025-55182	Meta	react-server-dom-webpack (“React2Shell”)	852	Critical
CVE-2025-14847	MongoDB Inc.	MongoDB Server	204	High
CVE-2025-20393	Cisco	Cisco Secure Email	89	Critical
CVE-2015-2051	D-Link	DIR-645	62	High
CVE-2017-18368	ZyXEL	P660HN-T1A	62	Critical
CVE-2025-14733	WatchGuard	Fireware OS	60	Critical
CVE-2025-66516	Apache Software Foundation	Apache Tika core	57	High

Vulnerability	Vendor	Product	Sightings	VLAI Severity
CVE-2018-10562	DASAN Networks	GPON Router	56	Critical
CVE-2025-40602	SonicWall	SMA1000	53	Medium
CVE-2025-59718	Fortinet	FortiSwitchManager	53	Critical

0.4 Known Exploited Vulnerabilities (CISA, CIRCL, EUVD)

KEV catalogs aggregated by Vulnerability-Lookup. The monthly reports formally introduced a dedicated *Known Exploited Vulnerabilities* section starting in **September 2025**. The entries below mirror what was published in each monthly report between September and December 2025. Earlier 2025 KEV additions (January–August) are tracked in the Known Exploited Vulnerabilities Catalogs from CISA, EUVD, and CIRCL.

0.4.1 CISA KEV

0.4.1.1 September 2025

CVE ID	Date Added	Vendor	Product	VLAI Severity
CVE-2025-59689	29/09/25	Cisco	IOS	Medium
CVE-2025-10035	29/09/25	Fortra	GoAnywhere MFT	Critical
CVE-2025-32463	29/09/25	Sudo project	Sudo	High
CVE-2021-21311	29/09/25	vrana	adminer	High
CVE-2025-20352	29/09/25	Cisco	IOS	High
CVE-2025-20333	25/09/25	Cisco	ASA Software	Critical
CVE-2025-20362	25/09/25	Cisco	ASA Software	Medium
CVE-2025-10585	23/09/25	Google	Chrome	High
CVE-2025-5086	11/09/25	Dassault Systèmes	DELMIA Apriso	Critical
CVE-2025-53690	04/09/25	Sitecore	Experience Manager (XM)	Critical
CVE-2025-48543	04/09/25	Google	Android	High

CVE ID	Date Added	Vendor	Product	VLAI Severity
CVE-2025-38352	04/09/25	Linux	Linux kernel	High
CVE-2023-50224	03/09/25	TP-Link	TL-WR841N	Medium
CVE-2025-9377	03/09/25	TP-Link Systems Inc.	Archer C7(EU) V2	High
CVE-2020-24363	02/09/25	TP-Link	TL-WA855RE	High

0.4.1.2 October 2025

CVE ID	Date Added	Vendor	Product	VLAI Severity
CVE-2025-41244	30/10/25	VMware	VCF operations	High
CVE-2025-24893	30/10/25	XWiki	xwiki-platform	Critical
CVE-2025-6205	28/10/25	Dassault Systèmes	DELMIA Apriso	Critical
CVE-2025-6204	28/10/25	Dassault Systèmes	DELMIA Apriso	High
CVE-2025-54236	24/10/25	Adobe	Commerce	Critical
CVE-2025-59287	24/10/25	Microsoft	Windows Server (WSUS)	Critical
CVE-2025-61932	22/10/25	MOTEX Inc.	Lanscope Endpoint Manager	Critical
CVE-2025-61884	20/10/25	Oracle Corporation	Oracle Configurator	High
CVE-2022-48503	20/10/25	Apple	macOS	High
CVE-2025-2746	20/10/25	Kentico	Xperience	Critical
CVE-2025-2747	20/10/25	Kentico	Xperience	Critical
CVE-2025-33073	20/10/25	Microsoft	Windows	High
CVE-2025-54253	15/10/25	Adobe	Experience Manager	Critical

CVE ID	Date Added	Vendor	Product	VLAI Severity
CVE-2025-47827	14/10/25	IGEL	IGEL OS	Medium
CVE-2025-6264	14/10/25	Rapid7	Velociraptor	Medium
CVE-2016-7836	14/10/25	Sky Co., LTD.	SKYSEA Client View	Critical
CVE-2025-59230	14/10/25	Microsoft	Windows	High
CVE-2025-24990	14/10/25	Microsoft	Windows	High
CVE-2021-43798	09/10/25	Grafana	Grafana	High
CVE-2025-27915	07/10/25	Zimbra	Collaboration	Medium
CVE-2010-3962	06/10/25	Microsoft	Internet Explorer	High
CVE-2025-61882	06/10/25	Oracle Corporation	Oracle Concurrent Processing (EBS)	Critical
CVE-2021-22555	06/10/25	Linux / NetApp	Linux kernel	High
CVE-2010-3765	06/10/25	Mozilla	Firefox	Critical
CVE-2021-43226	06/10/25	Microsoft	Windows	High
CVE-2011-3402	06/10/25	Microsoft	Windows	High
CVE-2013-3918	06/10/25	Microsoft	Windows	High
CVE-2025-4008	02/10/25	Smartbedded	MeteoBridge	Critical
CVE-2015-7755	02/10/25	Juniper	ScreenOS	Critical
CVE-2017-1000353	02/10/25	Jenkins	Jenkins	Critical
CVE-2014-6278	02/10/25	GNU	Bash	Critical
CVE-2025-21043	02/10/25	Samsung Mobile	Samsung Mobile Devices	High

0.4.1.3 November 2025

CVE ID	Date Added	Vendor	Product	VLAI Severity
CVE-2025-48703	04/11/25	centos-webpanel	CentOS Web Panel	Critical
CVE-2025-11371	04/11/25	Gladinet	CentreStack / TrioFox	Medium
CVE-2025-21042	10/11/25	Samsung Mobile	Samsung Mobile Devices	High
CVE-2025-9242	12/11/25	WatchGuard	Fireware OS	Critical
CVE-2025-62215	12/11/25	Microsoft	Windows	High
CVE-2025-12480	12/11/25	TrioFox	TrioFox	Critical
CVE-2025-64446	14/11/25	Fortinet	FortiWeb	Critical
CVE-2025-58034	18/11/25	Fortinet	FortiWeb	High
CVE-2025-13223	19/11/25	Google	Chrome	High
CVE-2025-61757	21/11/25	Oracle Corporation	Identity Manager	Critical
CVE-2021-26829	28/11/25	scadabr	scadabr	Medium

0.4.1.4 December 2025

CVE ID	Date Added	Vendor	Product	VLAI Severity
CVE-2025-14847	29/12/25	MongoDB Inc.	MongoDB Server	High
CVE-2023-52163	22/12/25	DigiEver	DS-2105 Pro	High
CVE-2025-14733	19/12/25	WatchGuard	Fireware OS	Critical
CVE-2025-20393	17/12/25	Cisco	Cisco Secure Email	Critical
CVE-2025-40602	17/12/25	SonicWall	SMA1000	Medium
CVE-2025-59374	17/12/25	ASUS	Live Update	Critical
CVE-2025-59718	16/12/25	Fortinet	FortiSwitchManager	Critical
CVE-2025-43529	15/12/25	Apple	iOS / iPadOS	High

CVE ID	Date Added	Vendor	Product	VLAI Severity
CVE-2025-14611	15/12/25	Gladinet	CentreStack / TrioFox	High
CVE-2025-14174	12/12/25	Google	Chrome	High
CVE-2018-4063	12/12/25	Sierra Wireless	ALEOS	High
CVE-2025-58360	11/12/25	GeoServer	GeoServer	High
CVE-2025-62221	09/12/25	Microsoft	Windows	High
CVE-2025-6218	09/12/25	RARLAB	WinRAR	High
CVE-2025-66644	08/12/25	Array Networks	ArrayOS AG	High
CVE-2022-37055	08/12/25	D-Link	GO-RT-AC750	Critical
CVE-2025-55182	05/12/25	Meta	react-server-dom-webpack	Critical
CVE-2021-26828	03/12/25	scadabr	scadabr	High
CVE-2025-48633	02/12/25	Google	Android	High
CVE-2025-48572	02/12/25	Google	Android	High

0.4.2 EUVD / ENISA KEV

0.4.2.1 September 2025

CVE ID	Date Added	Vendor	Product	VLAI Severity
CVE-2025-25231	09/09/25	Omnissa	Workspace ONE UEM	High

0.4.2.2 October, November, December 2025 No new entry was added to the EUVD / ENISA Known Exploited Vulnerabilities catalog during October, November and December 2025.

0.4.3 CIRCL KEV

The CIRCL Known Exploited Vulnerabilities catalog (`1a89b78e-f703-45f3-bb86-59eb712668bd`) tracks vulnerabilities that CIRCL has confirmed exploited based on its own incident-response, honey-

pot, and sinkhole telemetry. The entries below correspond to KEV records with confirmed exploitation activity observed during 2025:

CVE ID	Vendor	Product	First seen	Last seen	Evidence source
CVE-2023-28771	Zyxel	ZyWALL/USG, USG FLEX, ATP, VPN, ZLD firmware	2025-01-01	2026-01-28	CIRCL sinkhole (`cti-feed.circl.lu`)
CVE-2025-53770	Microsoft	SharePoint Server (“ToolShell”)	2025-07-20	2025-09-30	CIRCL incident response

The CIRCL KEV catalog remains intentionally small and high-confidence — every entry is backed by first-hand evidence collected by CIRCL — which is why its 2025 footprint is much narrower than the CISA KEV catalog.

0.5 Insights from Contributors

The following community comments and bundles were among the most relevant content shared on Vulnerability-Lookup during 2025.

0.5.1 January

- Unit42 Threat Brief: CVE-2025-0282 and CVE-2025-0283 — Ivanti Connect Secure exploitation analysis.
- CISA and FBI Release Advisory on How Threat Actors Chained Vulnerabilities in Ivanti Cloud Service Applications.
- Sonicwall vulnerabilities including critical ones.
- Haunted by Legacy: Discovering and Exploiting Vulnerable Tunnelling Hosts.
- 6 vulnerabilities in rsync server.
- CISA Releases Fact Sheet Detailing Embedded Backdoor Function of Contec CMS8000 Firmware.

0.5.2 February

- Black Basta’s Leaked Chat Logs — multi-vendor exploitation tracking from leaked Matrix chat logs.

- Update on SVR Cyber Operations and Vulnerability Exploitation.
- SonicWall Firewall Vulnerability Exploited After PoC Publication for CVE-2024-53704.
- Out-of-Cycle Security Bulletin: Juniper Session Smart Router auth bypass (CVE-2025-21589).
- Threat Actors Use CVE-2019-18935 to Deliver Reverse Shells.

0.5.3 March

- VMSA-2025-0004: VMware ESXi, Workstation, and Fusion updates address multiple vulnerabilities (CVE-2025-22224, CVE-2025-22225, CVE-2025-22226).
- Ingress NGINX Controller for Kubernetes — Vulnerabilities fixed in controller-v1.12.1.
- Kaspersky — Operation ForumTroll: APT attack with Google Chrome zero-day exploit chain.
- Pre-authentication SQL injection to RCE in GLPI (CVE-2025-24799/CVE-2025-24801).
- StopRansomware: Ghost (Cring) Ransomware | CISA.

0.5.4 April

- Suspected China-Nexus Threat Actor Actively Exploiting Critical Ivanti Connect Secure Vulnerability (CVE-2025-22457).
- CVE-2025-24054, NTLM Exploit in the Wild — Checkpoint Research.
- PHP Core Security Audit Results.
- Check if SAP system is vulnerable to CVE-2025-31324.
- Path Traversal Vulnerability in Surveillance Software — Luxembourg and Belgium notified.

0.5.5 May

- CVE-2025-22252: Authentication bypass in FortiOS, FortiProxy, and FortiSwitchManager.
- CVE-2025-30663: Zoom Workplace privilege escalation.
- CVE-2025-27920: Output Messenger exploited since April 2024.

0.5.6 June

- CitrixBleed 2 (CVE-2025-5777) — analysis comparing the flaw to CVE-2023-4966.
- GCVE-1-2025-0002: Cl0p ransomware data exfiltration utility vulnerable to RCE.
- Stuxnet-related CVEs.
- CVE-2025-31022: PayU WordPress plugin account takeover.
- CVE-2025-4517: CPython tarfile library RCE.

0.5.7 July

- Pre-Auth SQL Injection to RCE — Fortinet FortiWeb Fabric Connector (CVE-2025-25257).
- Ruckus network management solutions riddled with unpatched vulnerabilities.
- VMSA-2025-0013: VMware ESXi, Workstation, Fusion, and Tools updates.

0.5.8 August

- NetScaler ADC and NetScaler Gateway Security Bulletin (CVE-2025-7775, CVE-2025-7776, CVE-2025-8424).
- Citrix forgot to tell you CVE-2025-6543 has been used as a zero day since May 2025.
- Cache Me If You Can — Sitecore Experience Platform cache poisoning to RCE.

0.5.9 September

- SAP Security Patch Day — September 2025.
- npm.js — account `qix` and `duckdb_admin` compromised and associated CVEs allocated.
- Cisco AnyConnect/ASA — vulnerabilities.
- Subverting code integrity checks to locally backdoor Signal, 1Password, Slack, and more.

0.5.10 October

- F5 — K000156572: Quarterly Security Notification (October 2025).
- OpenSSL Security Advisory.
- Indicators of Compromise (IOCs) for CVE-2025-59287 (WSUS).
- Growing speculation that the Red Hat compromise may be linked to a recently disclosed vulnerability in Red Hat OpenShift AI.

0.5.11 November

- RCE in Agent DVR.
- Amazon discovers APT exploiting Cisco and Citrix zero-days.
- Suricata 8.0.2 and 7.0.13 released — including multiple vulnerabilities.
- UNC6148 Backdoors Fully-Patched SonicWall SMA 100 Series Devices with OVERSTEP Rootkit.

0.5.12 December

- React2Shell (CVE-2025-55182).
- The LAST Linux 5.4.y release. It is now end-of-life and should not be used by anyone, anymore..
- Apache Tika (CVE-2025-66516).
- Security content of iOS 26.2 and iPadOS 26.2.
- Reports About Cyberattacks Against Cisco Secure Email Gateway And Cisco Secure Email and Web Manager.

0.6 Thank you

A heartfelt thank you to all the contributors, source maintainers, and users who reported sightings, posted comments, curated bundles, and provided feedback throughout 2025. Vulnerability-Lookup is a community effort, and the depth of this year-in-review is a direct reflection of your engagement. Special thanks to the Shadowserver Foundation, the MISP project, the CISA KEV, the EUVD / ENISA team, and the many researchers who share information openly with the community.

If you want to contribute to the next report, you can create your account.

0.7 Feedback and Support

If you have suggestions, please feel free to open a ticket on our GitHub repository. Your feedback is invaluable to us: https://github.com/vulnerability-lookup/vulnerability-lookup/issues/

You can also explore and reuse the AI tooling that produced this report: **VulnMCP** — https://github.com/vulnerability-lookup/VulnMCP.

0.8 Funding

The main objective of the Federated European Team for Threat Analysis (FETTA) is the improvement of Cyber Threat Intelligence (CTI) products available to the public and private sectors in Poland, Luxembourg, and the European Union as a whole. Developing actionable CTI products (reports, indicators, etc.) is a complex task and requires an in-depth understanding of the threat landscape and the ability to analyse and interpret large amounts of data. Many SOCs and CSIRTs build their capabilities in this area independently, leading to a fragmented approach and duplication of work.

The Computer Incident Response Center Luxembourg (CIRCL) is a government-driven initiative designed to provide a systematic response facility to computer security threats and incidents. The organisation brings to the table its extensive experience in cybersecurity incident management, threat intelligence, and proactive response strategies. With a strong background in developing innovative open source cybersecurity tools and solutions, CIRCL's contribution to the FETTA project is instrumental in achieving enhanced collaboration and intelligence sharing across Europe.

Press release