



Scottish
Cyber
Coordination
Centre

Weekly Vulnerability Report

4 June 2024

This report summarizes the known software vulnerabilities published during the period **27 May-2 June 2024**. This data can help users prioritise and manage the vulnerabilities that might pose a risk to their organisations.

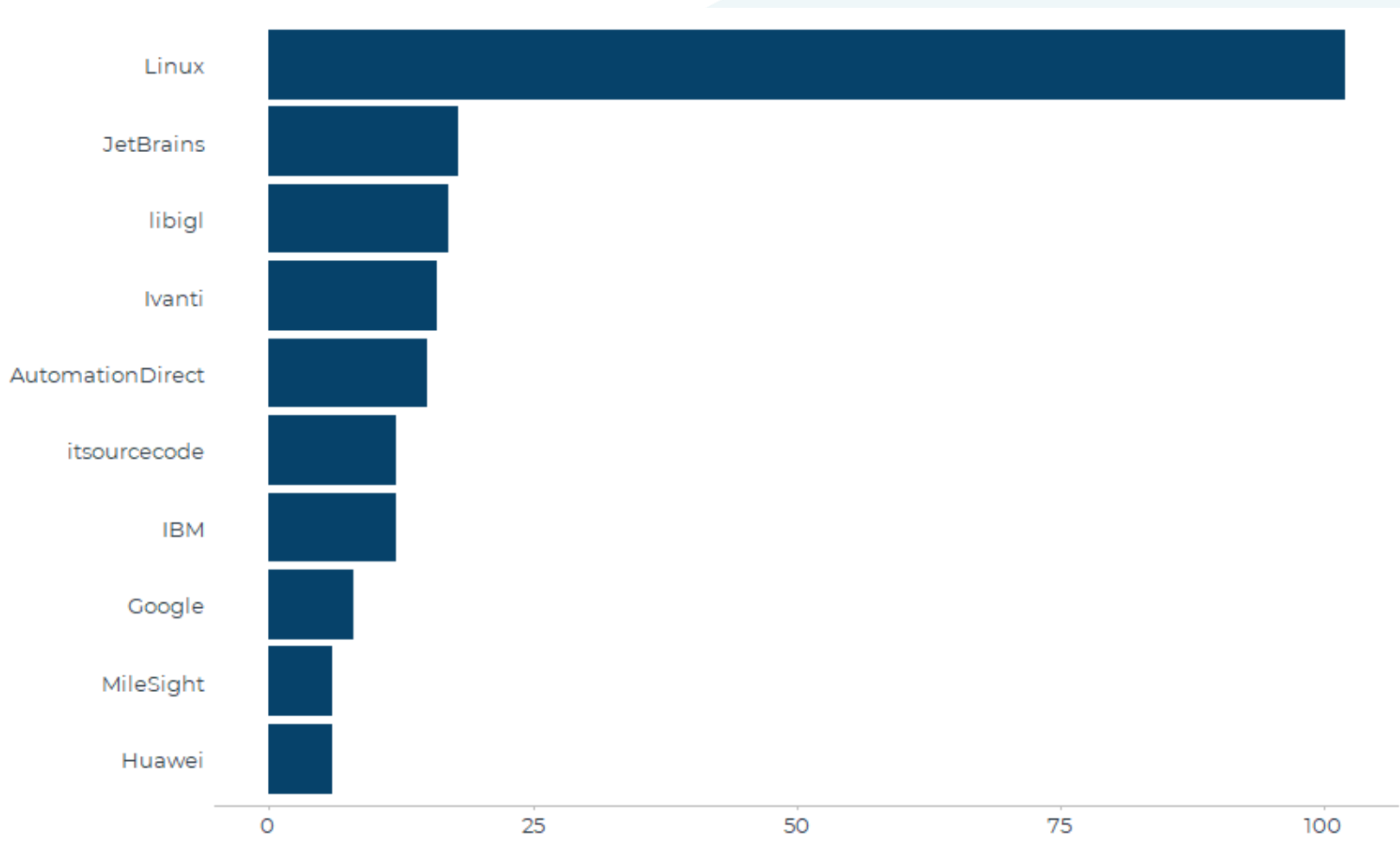
It includes a breakdown of vulnerabilities by vendor, a table of vulnerabilities with the highest likelihood of being exploited ([EPSS >0.001](#)), and a table of vulnerabilities with the highest severity rating ([CVSSv3 Base Score >=9](#)). The tables also indicate whether a vulnerability has been exploited according to the [CISA Known Exploited Catalog](#).

Each CVE number in the table has a link to the vendor advisory where users can find mitigation or remediation guidance.

We would like to know what you think about the weekly vulnerability report. Please take a few minutes to complete this anonymous [survey](#).



Count of vulnerabilities by software vendor (top 10), 27 May-2 June 2024





Vulnerabilities with highest likelihood of exploitation, 27 May-2 June 2024

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-24919	28-05-2024	checkpoint	Check Point Quantum Gateway, Spark Gateway and CloudGuard Network	8.6	0.945	Yes
CVE-2024-5274	28-05-2024	Google	Chrome	NA	0.014	Yes



Vulnerabilities with highest severity, 27 May-2 June 2024

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-3200	01-06-2024	tomdever	wpForo Forum	9.9		No
CVE-2024-21785	28-05-2024	AutomationDirect	P3-550E	9.8	0.001	No
CVE-2024-23601	28-05-2024	AutomationDirect	P3-550E	9.8	0.001	No
CVE-2024-23692	31-05-2024	Rejetto	HTTP File Server	9.8		No
CVE-2024-24962	28-05-2024	AutomationDirect	P3-550E	9.8	0.001	No
CVE-2024-24963	28-05-2024	AutomationDirect	P3-550E	9.8	0.001	No
CVE-2024-26289	27-05-2024	PMB Services	PMB	9.8		No
CVE-2024-27776	02-06-2024	MileSight	DeviceHub	9.8	NA	No
CVE-2024-3584	30-05-2024	qdrant	qdrant/qdrant	9.8		No
CVE-2024-36108	31-05-2024	casgate	casgate	9.8		No
CVE-2024-36389	02-06-2024	MileSight	DeviceHub	9.8	NA	No



CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-4358	29-05-2024	Progress Software Corporation	Telerik Report Server	9.8	0.001	No
CVE-2024-5150	29-05-2024	glboy	Login with phone number	9.8	0.001	No
CVE-2024-5514	30-05-2024	MinMax Digital Technology	MinMax CMS	9.8	0.001	No
CVE-2024-29822	31-05-2024	Ivanti	EPM	9.6	0.001	No
CVE-2024-29823	31-05-2024	Ivanti	EPM	9.6	0.001	No
CVE-2024-29824	31-05-2024	Ivanti	EPM	9.6	0.001	No
CVE-2024-29825	31-05-2024	Ivanti	EPM	9.6	0.001	No
CVE-2024-29826	31-05-2024	Ivanti	EPM	9.6	0.001	No
CVE-2024-29827	31-05-2024	Ivanti	EPM	9.6	0.001	No
CVE-2024-2421	30-05-2024	LenelS2	NetBox	9.3		No
CVE-2024-2422	30-05-2024	LenelS2	NetBox	9.3		No
CVE-2024-1275	31-05-2024	Baxter	Welch Ally Connex Spot Monitor	9.1		No



Scottish
Cyber
Coordination
Centre

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-22187	28-05-2024	AutomationDirect	P3-550E	9.1		No
CVE-2024-3412	29-05-2024	renehermi	WP STAGING WordPress Backup Plugin – Migration Backup Restore	9.1		No
CVE-2024-36391	02-06-2024	MileSight	DeviceHub	9.1	NA	No
CVE-2024-3300	30-05-2024	Dassault Systèmes	DELMIA Apriso	9		No



Scottish
Cyber
Coordination
Centre

About this data

This report brings together information from several sources including:

- CISA Known Exploited Vulnerabilities Catalog
- CVE Program
- FIRST - Exploit Prediction Scoring System (EPSS)

Note: The information in this report represents a snapshot in time and may become outdated by the time of publication as CVSS or EPSS scores are updated or new vulnerabilities are added to the Known Exploited Vulnerabilities Catalog.

For further information please contact SC3@gov.scot