Scottish Cyber Coordination Centre

Weekly Vulnerability Report

2 July 2024

This report summarizes the known software vulnerabilities published during the period **24-30 June 2024**. This data can help users prioritise and manage the vulnerabilities that might pose a risk to their organisations.

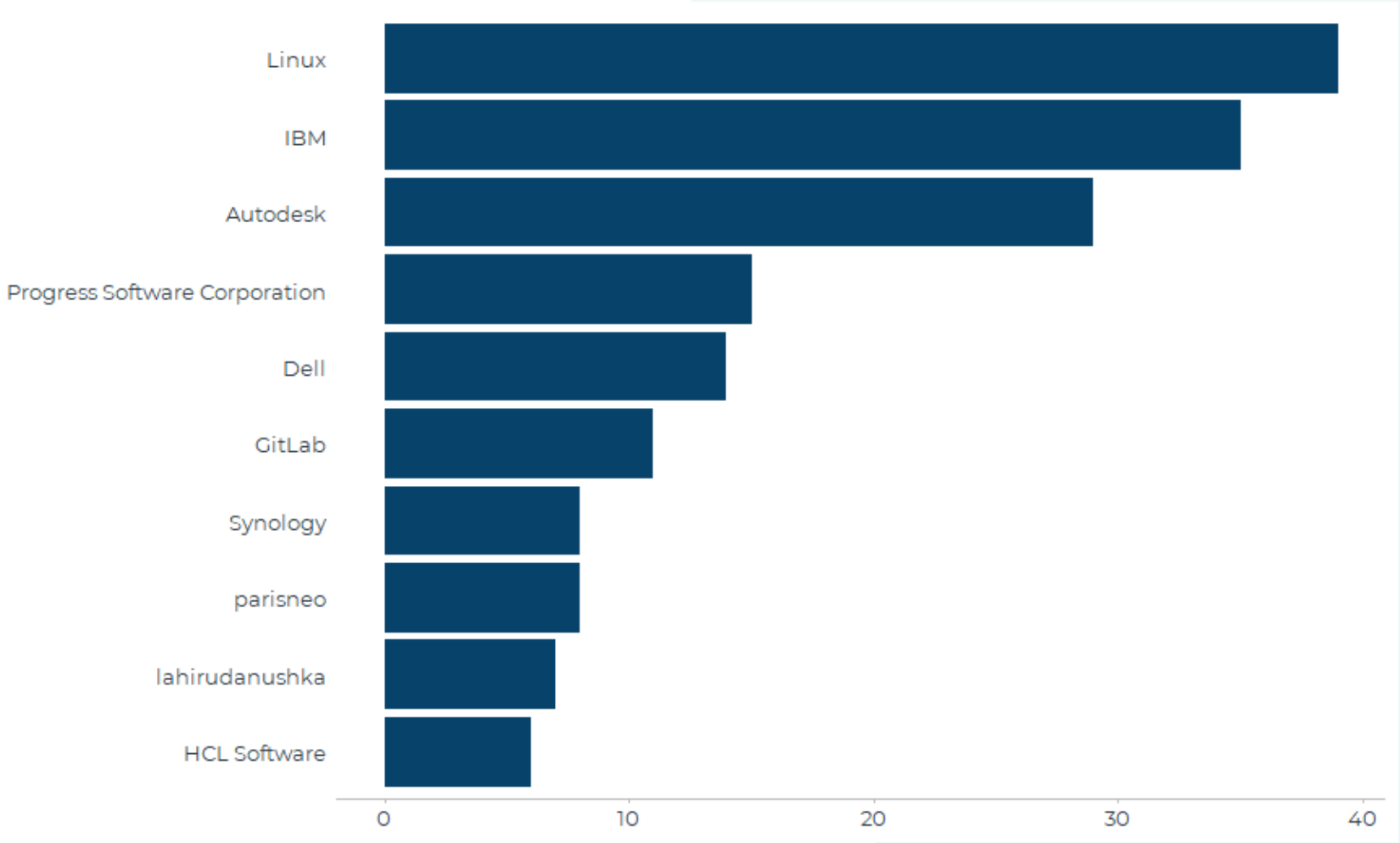
It includes a breakdown of vulnerabilities by vendor, a table of vulnerabilities with the highest likelihood of being exploited (EPSS >0.001), and a table of vulnerabilities with the highest severity rating (CVSSv3 Base Score >=9). The tables also indicate whether a vulnerability has been exploited according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

Scottish Cyber Coordination Centre

Count of vulnerabilities by software vendor (top 10), 24-30 June 2024



Scottish Cyber Coordination Centre

Vulnerabilities with highest likelihood of exploitation, 24-30 June 2024

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-6297	25-06-2024	warfareplugins	Social Sharing Plugin – Social Warfare	10	0.001	No
CVE-2024-23147	25-06-2024	Autodesk	AutoCAD, Advance Steel and Civil 3D	8.8	0.001	No
CVE-2024-23156	25-06-2024	Autodesk	AutoCAD, Advance Steel and Civil 3D	7.8	0.001	No
CVE-2024-23157	25-06-2024	Autodesk	AutoCAD, Advance Steel and Civil 3D	8.8	0.001	No
CVE-2024-37000	25-06-2024	Autodesk	AutoCAD, Advance Steel and Civil 3D	8.8	0.001	No
CVE-2024-37006	25-06-2024	Autodesk	AutoCAD, Advance Steel and Civil 3D	8.8	0.001	No
CVE-2024-6323	26-06-2024	GitLab	GitLab	7.5	0.001	No

Scottish Cyber Coordination Centre

Vulnerabilities with highest severity, 24-30 June 2024

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-3330	27-06-2024	Spotfire	Spotfire Analyst	9.9		No
CVE-2024-37091	24-06-2024	StylemixThemes	Consulting Elementor Widgets	9.9		No
CVE-2024-37109	24-06-2024	Membership Software	WishList Member X	9.9		No
CVE-2024-4197	25-06-2024	Avaya	IP Office	9.9		No
CVE-2024-6303	25-06-2024	The Conduit Contributors	Conduit	9.9		No
CVE-2024-0947	27-06-2024	Talya Informatics	Elektraweb	9.8	0.001	No
CVE-2024-0949	27-06-2024	Talya Informatics	Elektraweb	9.8	0.001	No
CVE-2024-21741	25-06-2024	n/a	n/a	9.8		No
CVE-2024-33278	24-06-2024	n/a	n/a	9.8		No
CVE-2024-34313	24-06-2024	n/a	n/a	9.8		No
CVE-2024-34988	24-06-2024	n/a	n/a	9.8		No

Scottish Cyber Coordination Centre

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-36681	24-06-2024	n/a	n/a	9.8		No
CVE-2024-37734	26-06-2024	n/a	n/a	9.8		No
CVE-2024-37759	24-06-2024	n/a	n/a	9.8		No
CVE-2024-38902	24-06-2024	n/a	n/a	9.8		No
CVE-2024-39243	26-06-2024	n/a	n/a	9.8		No
CVE-2024-39349	28-06-2024	Synology	Camera Firmware	9.8		No
CVE-2024-39462	25-06-2024	Linux	Linux	9.8		No
CVE-2024-39669	27-06-2024	n/a	n/a	9.8		No
CVE-2024-39705	27-06-2024	n/a	n/a	9.8		No
CVE-2024-4228	26-06-2024	Magarsus Consultancy	SSO (Single Sign On)	9.8	0.001	No
CVE-2024-4883	25-06-2024	Progress Software Corporation	WhatsUp Gold	9.8		No

Scottish Cyber Coordination Centre

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-4884	25-06-2024	Progress Software Corporation	WhatsUp Gold	9.8		No
CVE-2024-4885	25-06-2024	Progress Software Corporation	WhatsUp Gold	9.8		No
CVE-2024-5181	26-06-2024	mudler	mudler/localai	9.8		No
CVE-2024-5276	25-06-2024	Fortra	FileCatalyst Workflow	9.8		No
CVE-2024-5683	24-06-2024	Next4Biz CRM & BPM Software	Business Process Manangement (BPM)	9.8	0.001	No
CVE-2024-5751	27-06-2024	berriai	berriai/litellm	9.8		No
CVE-2024-5826	27-06-2024	vanna-ai	vanna-ai/vanna	9.8		No
CVE-2024-5827	28-06-2024	vanna-ai	vanna-ai/vanna	9.8		No
CVE-2024-6028	25-06-2024	ays-pro	Quiz Maker	9.8	0.001	No
CVE-2024-6127	27-06-2024	BC Security	Empire	9.8		No
CVE-2024-6265	29-06-2024	stiofansisland	UsersWP – Front-end login form, User Registration, User Profile &	9.8	0.001	No

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
			Members Directory plugin for WordPress			
CVE-2024-38373	24-06-2024	FreeRTOS	FreeRTOS-Plus-TCP	9.6		No
CVE-2024-5655	26-06-2024	GitLab	GitLab	9.6	0.001	No
CVE-2023-6198	25-06-2024	Baicells	Snap Router	9.3		No
CVE-2024-2882	27-06-2024	SDG Technologies	PnPSCADA	9.3		No
CVE-2024-37252	26-06-2024	Icegram	Email Subscribers & Newsletters	9.3		No
CVE-2024-39373	27-06-2024	marKoni	Markoni-D (Compact) FM Transmitters	9.3		No
CVE-2024-39374	27-06-2024	marKoni	Markoni-D (Compact) FM Transmitters	9.3		No
CVE-2024-39375	27-06-2024	marKoni	Markoni-D (Compact) FM Transmitters	9.3		No
CVE-2024-39376	27-06-2024	marKoni	Markoni-D (Compact) FM Transmitters	9.3		No
CVE-2024-5988	25-06-2024	Rockwell Automation	ThinManager® ThinServer™	9.3		No
CVE-2024-5989	25-06-2024	Rockwell Automation	ThinManager® ThinServer™	9.3		No

Scottish Cyber Coordination Centre

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-6060	25-06-2024	Phloc	Webscopes	9.3		No
CVE-2024-6160	24-06-2024	Jan Syski	MegaBIP	9.3		No
CVE-2024-29039	28-06-2024	tpm2-software	tpm2-tools	9.1		No
CVE-2024-29868	24-06-2024	Apache Software Foundation	Apache StreamPipes	9.1		No
CVE-2024-36497	24-06-2024	Faronics	WINSelect (Standard + Enterprise)	9.1		No
CVE-2024-5535	27-06-2024	OpenSSL	OpenSSL	9.1		No
CVE-2024-5805	25-06-2024	Progress	MOVEit Gateway	9.1		No
CVE-2024-5806	25-06-2024	Progress	MOVEit Transfer	9.1		No
CVE-2024-5980	27-06-2024	lightning-ai	lightning-ai/pytorch-lightning	9.1		No
CVE-2024-37089	24-06-2024	StylemixThemes	Consulting Elementor Widgets	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