Scottish Cyber Coordination Centre

Weekly Vulnerability Report

16 April 2024

This report summarizes the known software vulnerabilities published during the period **8-14 April 2024**. This data can help users prioritise and manage the vulnerabilities that might pose a risk to their organisations.

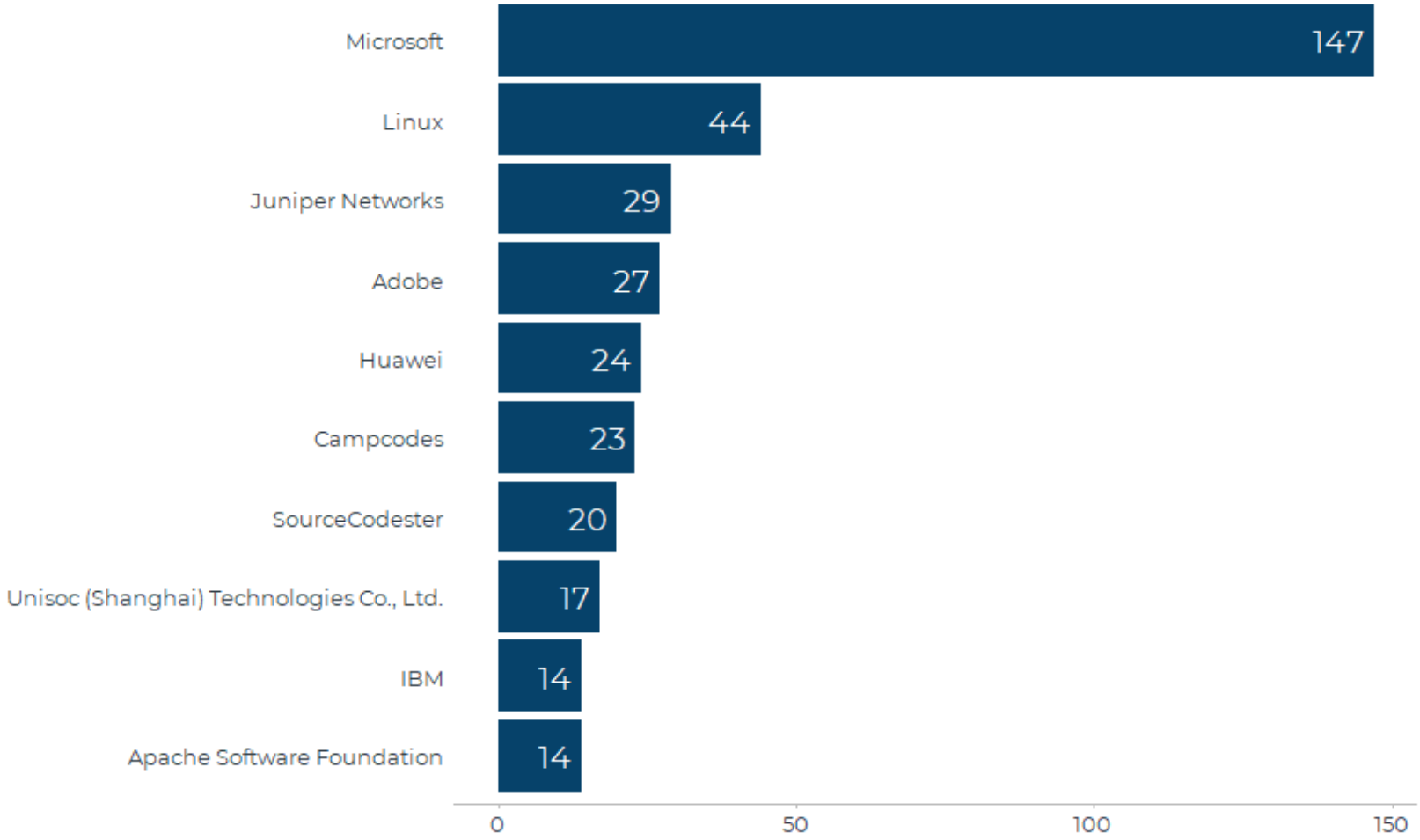
It includes a breakdown of vulnerabilities by vendor, a table of vulnerabilities with the highest likelihood of being exploited (EPSS >0.002), and a table of vulnerabilities with the highest severity rating (CVSSv3 Base Score >=9). The tables also indicate whether a vulnerability has been exploited according 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), 8-14 April 2024



Scottish Cyber Coordination Centre

Vulnerabilities with highest likelihood of exploitation, 8-14 April 2024

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-3400	12-04-2024	Palo Alto Networks	PAN-OS	10	0.004	Yes

Scottish Cyber Coordination Centre

Vulnerabilities with highest severity, 8-14 April 2024

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-3025	10-04-2024	mintplex-labs	mintplex-labs/anything-llm	9.9		No
CVE-2023-1083	09-04-2024	Welotec	TK515L	9.8		No
CVE-2024-1511	10-04-2024	parisneo	parisneo/lollms-webui	9.8		No
CVE-2024-1520	10-04-2024	parisneo	parisneo/lollms-webui	9.8		No
CVE-2024-1813	09-04-2024	presstigers	Simple Job Board	9.8		No
CVE-2024-2029	10-04-2024	mudler	mudler/localai	9.8		No
CVE-2024-21508	11-04-2024	n/a	mysql2	9.8		No
CVE-2024-2195	10-04-2024	aimhubio	aimhubio/aim	9.8		No
CVE-2024-2221	10-04-2024	qdrant	qdrant/qdrant	9.8		No
CVE-2024-2804	09-04-2024	jokr	Network Summary	9.8		No
CVE-2024-2952	10-04-2024	berriai	berriai/litellm	9.8		No

Scottish Cyber Coordination Centre

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-29836	14-04-2024	CS Technologies Australia	Evolution Controller	9.8		No
CVE-2024-3098	10-04-2024	run-llama	run-llama/llama_index	9.8		No
CVE-2024-31224	08-04-2024	binary-husky	gpt_academic	9.8		No
CVE-2024-3136	09-04-2024	stylemix	MasterStudy LMS WordPress Plugin – for Online Courses and Education	9.8		No
CVE-2024-3704	12-04-2024	OpenGnsys	OpenGnsys	9.8		No
CVE-2024-3765	14-04-2024	Xiongmai	AHB7804R-MH-V2	9.8		No
CVE-2024-31214	10-04-2024	traccar	traccar	9.7		No
CVE-2024-31988	10-04-2024	xwiki	xwiki-platform	9.7		No
CVE-2024-28878	12-04-2024	IOSiX	IO-1020 Micro ELD	9.6		No
CVE-2023-45590	09-04-2024	Fortinet	FortiClientLinux	9.4		No
CVE-2024-1600	10-04-2024	parisneo	parisneo/lollms-webui	9.3		No

Scottish Cyber Coordination Centre

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2023-6318	09-04-2024	LG	webOS	9.1		No
CVE-2023-6319	09-04-2024	LG	webOS	9.1		No
CVE-2023-6320	09-04-2024	LG	webOS	9.1		No
CVE-2024-1643	10-04-2024	lunary-ai	lunary-ai/lunary	9.1		No
CVE-2024-1740	10-04-2024	lunary-ai	lunary-ai/lunary	9.1		No
CVE-2024-1741	10-04-2024	lunary-ai	lunary-ai/lunary	9.1		No
CVE-2024-31461	10-04-2024	makeplane	plane	9.1		No
CVE-2024-31986	10-04-2024	xwiki	xwiki-platform	9.1		No
CVE-2024-20758	10-04-2024	Adobe	Adobe Commerce	9		No
CVE-2024-29990	09-04-2024	Microsoft	Azure Kubernetes Service	9		No
CVE-2024-3119	09-04-2024	irontec	sngrep	9		No
CVE-2024-3120	09-04-2024	irontec	sngrep	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