



Scottish
Cyber
Coordination
Centre

Weekly Vulnerability Report

21 May 2024

This report summarizes the known software vulnerabilities published during the period **13-19 May 2024**. This data can help users prioritise and manage the vulnerabilities that might pose a risk to their organisations.

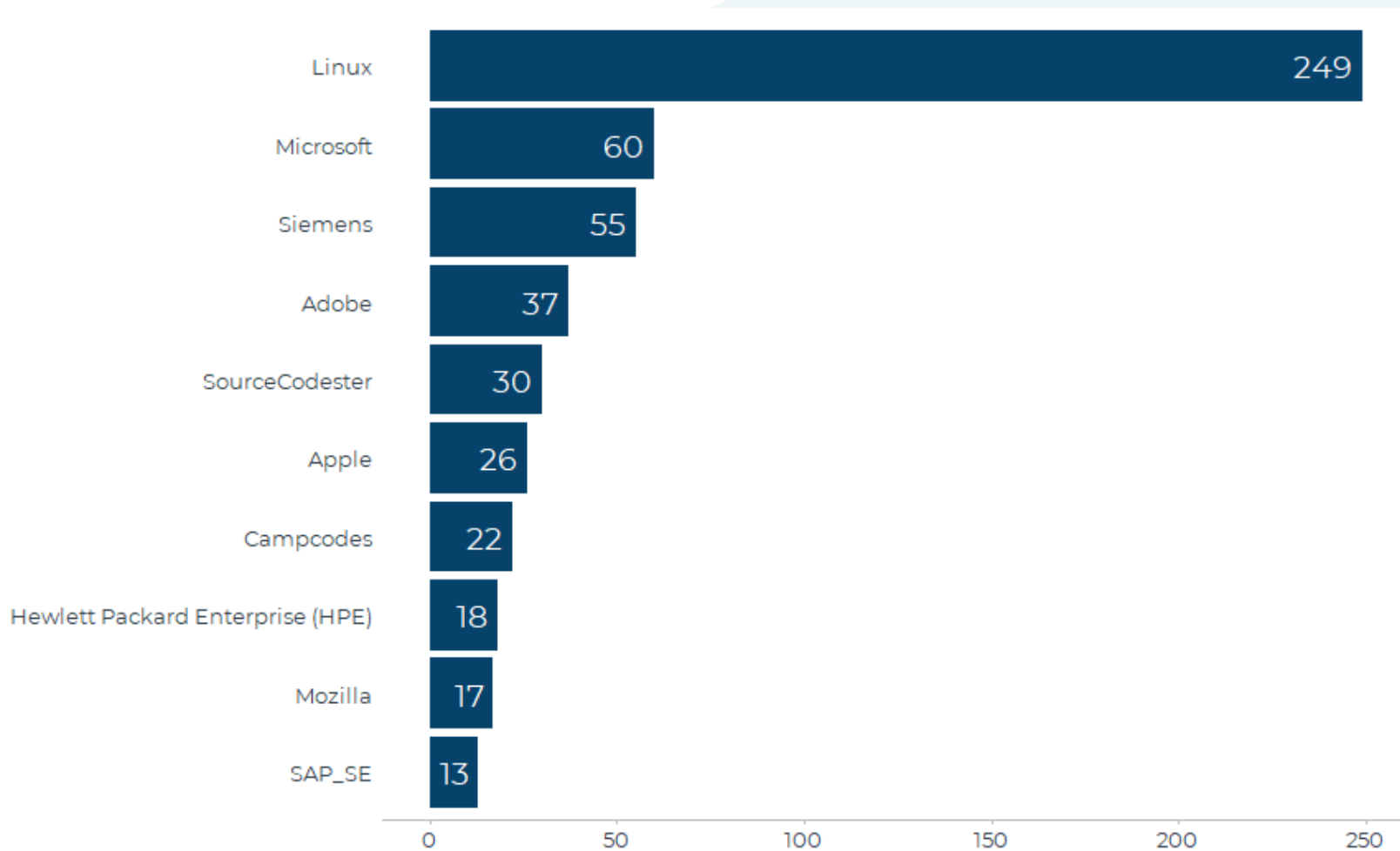
It includes a breakdown of vulnerabilities by vendor, a table of vulnerabilities with the highest likelihood of being exploited (**EPSS >0.001**), and a table of vulnerabilities with the highest severity rating (**CVSSv3 Base Score >=9**). The tables also indicate whether a vulnerability has been exploited 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), 13-19 May 2024





Vulnerabilities with highest likelihood of exploitation, 13-19 May 2024

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-4761	14-05-2024	Google	Chrome	NA	0.045	Yes
CVE-2024-30040	14-05-2024	Microsoft	Windows 10 Version 1809	8.8	0.009	Yes
CVE-2024-30054	14-05-2024	Microsoft	PowerBI-client JS SDK	6.5	0.001	No



Vulnerabilities with highest severity, 13-19 May 2024

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2023-23645	17-05-2024	MainWP	MainWP Code Snippets Extension	9.9		No
CVE-2024-29212	13-05-2024	Veeam	Service Provider Console	9.9		No
CVE-2024-33644	17-05-2024	WPCustomify	Customify Site Library	9.9		No
CVE-2024-34411	13-05-2024	Thomas Scholl	canvasio3D Light	9.9		No
CVE-2023-25701	17-05-2024	WhatArmy	WatchTowerHQ	9.8		No
CVE-2023-26009	17-05-2024	Favethemes	Houzez Login Register	9.8		No
CVE-2023-26540	17-05-2024	Favethemes	Houzez	9.8		No
CVE-2023-32244	17-05-2024	XTemos	Woodmart Core	9.8		No
CVE-2023-37999	17-05-2024	HasThemes	HT Mega	9.8		No
CVE-2023-51424	17-05-2024	Saleswonder Team	WebinarIgnition	9.8		No
CVE-2023-51476	17-05-2024	IOSS	WP MLM Unilevel	9.8		No



CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2023-51481	17-05-2024	powerfulwp	Local Delivery Drivers for WooCommerce	9.8		No
CVE-2023-51483	17-05-2024	Glowlogix	WP Frontend Profile	9.8		No
CVE-2024-22157	17-05-2024	WebWizards	SalesKing	9.8		No
CVE-2024-2358	16-05-2024	parisneo	parisneo/lollms-webui	9.8		No
CVE-2024-24882	17-05-2024	Masteriyo	LMS	9.8		No
CVE-2024-2771	18-05-2024	techjewel	Contact Form Plugin by Fluent Forms for Quiz, Survey, and Drag & Drop WP Form Builder	9.8	0.001	No
CVE-2024-27939	14-05-2024	Siemens	RUGGEDCOM CROSSBOW	9.8		No
CVE-2024-30542	17-05-2024	Wholesale	WholesaleX	9.8		No
CVE-2024-31290	17-05-2024	CodeRevolution	Demo My WordPress	9.8		No
CVE-2024-31466	14-05-2024	Hewlett Packard Enterprise (HPE)	Aruba InstantOS and Aruba Access Points running ArubaOS 10	9.8		No



CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-31467	14-05-2024	Hewlett Packard Enterprise (HPE)	Aruba InstantOS and Aruba Access Points running ArubaOS 10	9.8		No
CVE-2024-31468	14-05-2024	Hewlett Packard Enterprise (HPE)	Aruba InstantOS and Aruba Access Points running ArubaOS 10	9.8		No
CVE-2024-31469	14-05-2024	Hewlett Packard Enterprise (HPE)	Aruba InstantOS and Aruba Access Points running ArubaOS 10	9.8		No
CVE-2024-31470	14-05-2024	Hewlett Packard Enterprise (HPE)	Aruba InstantOS and Aruba Access Points running ArubaOS 10	9.8		No
CVE-2024-31471	14-05-2024	Hewlett Packard Enterprise (HPE)	Aruba InstantOS and Aruba Access Points running ArubaOS 10	9.8		No
CVE-2024-31472	14-05-2024	Hewlett Packard Enterprise (HPE)	Aruba InstantOS and Aruba Access Points running ArubaOS 10	9.8		No



CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-31473	14-05-2024	Hewlett Packard Enterprise (HPE)	Aruba InstantOS and Aruba Access Points running ArubaOS 10	9.8		No
CVE-2024-32047	15-05-2024	CyberPower	PowerPanel business	9.8		No
CVE-2024-32053	15-05-2024	CyberPower	PowerPanel business	9.8		No
CVE-2024-32511	17-05-2024	Astoundify	Simple Registration for WooCommerce	9.8		No
CVE-2024-3263	13-05-2024	YMS	VIS Pro	9.8		No
CVE-2024-32740	14-05-2024	Siemens	SIMATIC CN 4100	9.8		No
CVE-2024-33552	17-05-2024	8theme	XStore Core	9.8		No
CVE-2024-33567	17-05-2024	UkrSolution	Barcode Scanner with Inventory & Order Manager	9.8		No
CVE-2024-33625	15-05-2024	CyberPower	PowerPanel business	9.8		No
CVE-2024-34025	15-05-2024	CyberPower	PowerPanel business	9.8		No
CVE-2024-34706	13-05-2024	valtimo-platform	valtimo-frontend-libraries	9.8		No



CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-3658	18-05-2024	hakeemnala	Build App Online	9.8	0.001	No
CVE-2024-4078	16-05-2024	parisneo	parisneo/lollms	9.8		No
CVE-2024-4223	16-05-2024	themeum	Tutor LMS – eLearning and online course solution	9.8	0.001	No
CVE-2024-4326	16-05-2024	parisneo	parisneo/lollms-webui	9.8		No
CVE-2024-4824	13-05-2024	AROX SOLUTION	School ERP Pro+Responsive	9.8		No
CVE-2024-4825	13-05-2024	Agentejo	Cockpit CMS	9.8		No
CVE-2024-4893	15-05-2024	DigiWin	EasyFlow .NET	9.8	0.001	No
CVE-2024-4991	16-05-2024	SiAdmin	SiAdmin	9.8		No
CVE-2024-4992	16-05-2024	SiAdmin	SiAdmin	9.8		No
CVE-2024-34716	14-05-2024	PrestaShop	PrestaShop	9.7		No
CVE-2024-2361	16-05-2024	parisneo	parisneo/lollms-webui	9.6		No
CVE-2024-27107	14-05-2024	GE HealthCare	EchoPAC Software Only	9.6		No



CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-30209	14-05-2024	Siemens	SIMATIC RTLS Locating Manager	9.6		No
CVE-2024-33006	14-05-2024	SAP_SE	SAP NetWeaver Application Server ABAP and ABAP Platform	9.6		No
CVE-2024-4999	16-05-2024	Ligowave	UNITY	9.4		No
CVE-2024-22267	14-05-2024	NA	VMware Workstation	9.3		No
CVE-2024-27954	17-05-2024	WP Automatic	Automatic	9.3	0.001	No
CVE-2024-30314	16-05-2024	Adobe	Dreamweaver Desktop	9.3		No
CVE-2024-4826	16-05-2024	Asaancart	Simple PHP Shopping Cart	9.3		No
CVE-2024-5023	16-05-2024	Netflix	ConsoleMe	9.3		No
CVE-2023-25444	17-05-2024	JS Help Desk	JS Help Desk – Best Help Desk & Support Plugin	9.1		No
CVE-2024-22120	17-05-2024	Zabbix	Zabbix	9.1		No
CVE-2024-25641	13-05-2024	Cacti	cacti	9.1		No



CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-32002	14-05-2024	git	git	9.1		No
CVE-2024-3319	15-05-2024	SailPoint	Identity Security Cloud	9.1		No
CVE-2024-33499	14-05-2024	Siemens	SIMATIC RTLS Locating Manager	9.1		No
CVE-2024-34340	13-05-2024	Cacti	cacti	9.1	0.001	No
CVE-2024-34416	13-05-2024	NA	Pk Favicon Manager	9.1		No
CVE-2024-34440	13-05-2024	Jordy Meow	AI Engine: ChatGPT Chatbot	9.1		No
CVE-2024-34555	13-05-2024	URBAN BASE	Z-Downloads	9.1		No
CVE-2024-35187	16-05-2024	stalwartlabs	mail-server	9.1		No
CVE-2023-32297	17-05-2024	LWS	LWS Affiliation	9		No
CVE-2024-2366	16-05-2024	parisneo	parisneo/lollms-webui	9		No
CVE-2024-31231	17-05-2024	Sizam Design	Rehub	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