



Scottish
Cyber
Coordination
Centre

Weekly Vulnerability Report

30 April 2024

This report summarizes the known software vulnerabilities published during the period **22-28 April 2024**. This data can help users prioritise and manage the vulnerabilities that might pose a risk to their organisations.

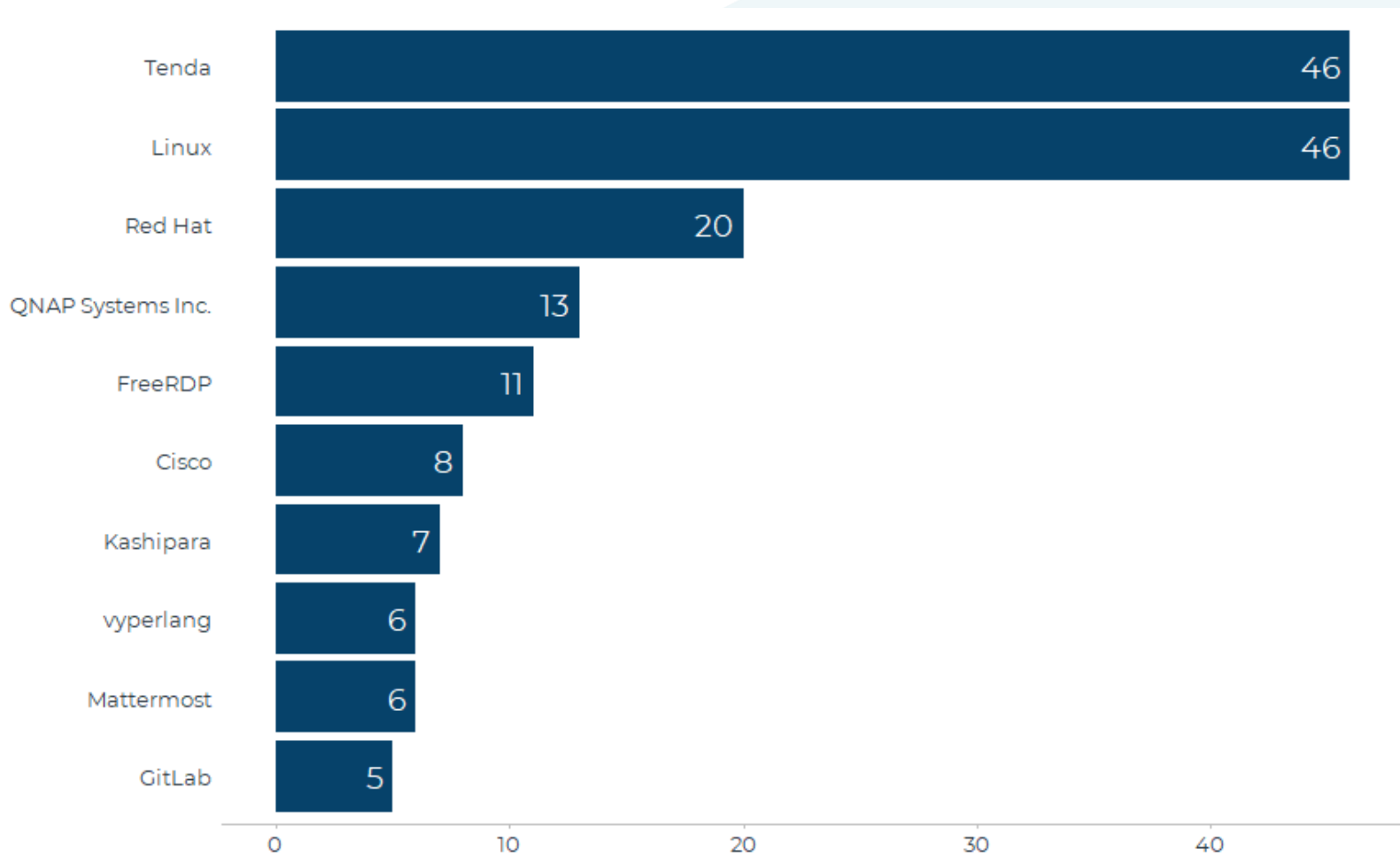
It includes a breakdown of vulnerabilities by vendor, a table of vulnerabilities with the highest likelihood of being exploited (**EPSS >0.001**), and a table of vulnerabilities with the highest severity rating (**CVSSv3 Base Score >=9**). The tables also indicate whether a vulnerability has been exploited 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), 22-28 April 2024





Vulnerabilities with highest likelihood of exploitation, 22-28 April 2024

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-4040	22-04-2024	CrushFTP	CrushFTP	9.8	0.016	Yes
CVE-2024-20353	24-04-2024	Cisco	Cisco Adaptive Security Appliance (ASA) Software	8.6	0.002	Yes
CVE-2024-20359	24-04-2024	Cisco	Cisco Adaptive Security Appliance (ASA) Software	6	0.001	Yes



Vulnerabilities with highest severity, 22-28 April 2024

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2023-31090	24-04-2024	Unlimited Elements	Unlimited Elements For Elementor (Free Widgets, Addons, Templates)	9.9		No
CVE-2023-51482	25-04-2024	EazyPlugins	Eazy Plugin Manager	9.9		No
CVE-2024-32764	26-04-2024	QNAP Systems Inc.	myQNAPcloud Link	9.9		No
CVE-2024-3342	27-04-2024	jetmonsters	Timetable and Event Schedule by MotoPress	9.9		No
CVE-2023-51425	24-04-2024	Jacques Malgrange	Rencontre – Dating Site	9.8		No
CVE-2023-51472	24-04-2024	Mestres do WP	Checkout Mestres WP	9.8		No
CVE-2023-51477	24-04-2024	BUDDYBOSS DMCC	BuddyBoss Theme	9.8		No
CVE-2023-51478	25-04-2024	Abdul Hakeem	Build App Online	9.8		No
CVE-2023-51484	25-04-2024	wp-buy	Login as User or Customer (User Switching)	9.8		No
CVE-2024-0740	26-04-2024	Eclipse Foundation	Eclipse Target Management	9.8		No



CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-21511	23-04-2024	n/a	mysql2	9.8		No
CVE-2024-32039	22-04-2024	FreeRDP	FreeRDP	9.8		No
CVE-2024-32041	22-04-2024	FreeRDP	FreeRDP	9.8		No
CVE-2024-32458	22-04-2024	FreeRDP	FreeRDP	9.8		No
CVE-2024-32459	22-04-2024	FreeRDP	FreeRDP	9.8		No
CVE-2024-32658	23-04-2024	FreeRDP	FreeRDP	9.8		No
CVE-2024-32659	23-04-2024	FreeRDP	FreeRDP	9.8		No
CVE-2024-32881	26-04-2024	danswer-ai	danswer	9.8		No
CVE-2024-3962	26-04-2024	themeisle	Product Addons & Fields for WooCommerce	9.8		No
CVE-2024-4040	22-04-2024	CrushFTP	CrushFTP	9.8	0.016	Yes
CVE-2023-47222	26-04-2024	QNAP Systems Inc.	Media Streaming add-on	9.6		No
CVE-2024-30560	25-04-2024	大狭WP	DX-Watermark	9.6		No



CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-32709	24-04-2024	Plechev Andrey	WP-Recall	9.3		No
CVE-2022-36028	25-04-2024	bigbluebutton	greenlight	9.1	0.001	No
CVE-2022-36029	25-04-2024	bigbluebutton	greenlight	9.1	0.001	No
CVE-2024-31266	25-04-2024	AlgolPlus	Advanced Order Export For WooCommerce	9.1		No
CVE-2024-32836	24-04-2024	WP Lab	WP-Lister Lite for eBay	9.1		No
CVE-2024-32880	26-04-2024	payload	payload	9.1		No
CVE-2024-32948	24-04-2024	Repute Infosystems	ARMember	9.1		No
CVE-2024-32954	24-04-2024	Tribulant	Newsletters	9.1		No
CVE-2024-22144	25-04-2024	Eli Scheetz	Anti-Malware Security and Brute-Force Firewall	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