Scottish Cyber Coordination Centre

Weekly Vulnerability Report

2 April 2024

This report summarizes the known software vulnerabilities published during the period **25-31 March 2024**. This data can help users prioritise and manage the vulnerabilities that might pose a risk to their organisations.

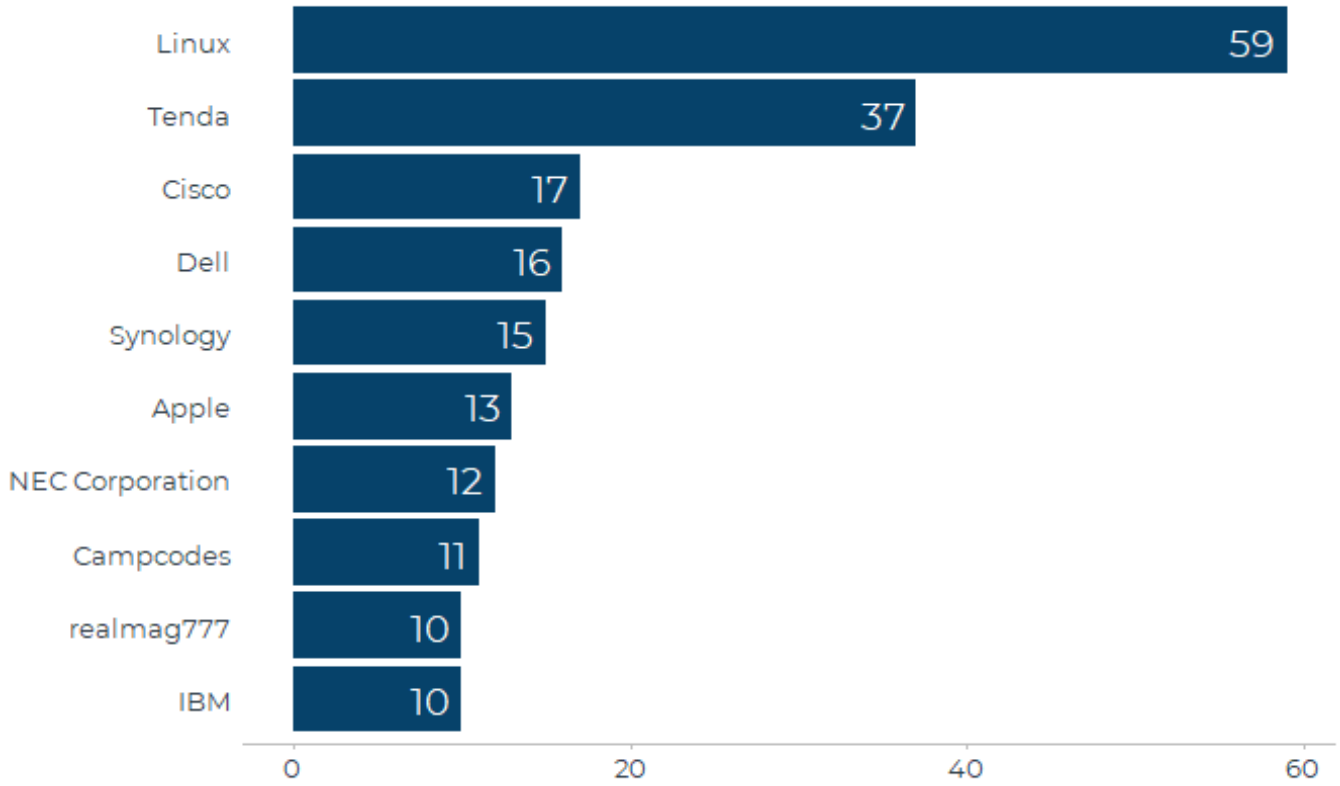
It includes a breakdown of vulnerabilities by vendor and a table of vulnerabilities with the highest severity rating (CVSSv3 Base Score >=9). This table also indicate whether a vulnerability has been exploited according to the CISA Known Exploited Catalog.

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), 25-31 March 2024



Scottish Cyber Coordination Centre

Vulnerabilities with highest severity, 25-31 March 2024

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2022-36407	25-03-2024	Hitachi	Hitachi Virtual Storage Platform	9.9		No
CVE-2023-46808	31-03-2024	Ivanti	ITSM	9.9		No
CVE-2023-48777	26-03-2024	Elementor.com	Elementor Website Builder	9.9	0.001	No
CVE-2024-29241	28-03-2024	Synology	Surveillance Station	9.9		No
CVE-2024-30228	28-03-2024	Hercules Design	Hercules Core	9.9		No
CVE-2024-30500	29-03-2024	CubeWP	CubeWP – All-in-One Dynamic Content Framework	9.9		No
CVE-2023-6153	27-03-2024	TeoSOFT Software	TeoBASE	9.8		No
CVE-2023-6173	27-03-2024	TeoSOFT Software	TeoBASE	9.8		No
CVE-2023-6191	29-03-2024	Egehan Security	WebPDKS	9.8		No
CVE-2023-6437	28-03-2024	TP-Link	TP-Link EX20v AX1800, Tp-Link Archer C5v AC1200, Tp-Link TD-W9970, Tp-Link TD-W9970v3, TP-Link VX220-G2u, TP-Link VN020-G2u	9.8		No

Scottish Cyber Coordination Centre

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-2409	29-03-2024	stylemix	MasterStudy LMS WordPress Plugin – for Online Courses and Education	9.8		No
CVE-2024-2411	29-03-2024	stylemix	MasterStudy LMS WordPress Plugin – for Online Courses and Education	9.8		No
CVE-2024-2865	25-03-2024	Mergen Software	Quality Management System	9.8		No
CVE-2023-41724	31-03-2024	Ivanti	Sentry	9.6		No
CVE-2023-28787	26-03-2024	ExpressTech	Quiz And Survey Master	9.3		No
CVE-2024-30490	29-03-2024	Metagauss	ProfileGrid	9.3		No
CVE-2024-30498	29-03-2024	CRM Perks	CRM Perks Forms	9.3		No
CVE-2024-30502	29-03-2024	WP Travel Engine	WP Travel Engine	9.3		No
CVE-2023-29386	26-03-2024	Julien Crego	Manager for Icomoon	9.1		No
CVE-2023-47842	26-03-2024	Zachary Segal	CataBlog	9.1		No
CVE-2023-47846	26-03-2024	Terry Lin	WP Githuber MD	9.1		No
CVE-2023-47873	26-03-2024	WEN Solutions	WP Child Theme Generator	9.1		No

Scottish Cyber Coordination Centre

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-2862	25-03-2024	LG Electronics	LG LED Assistant	9.1		No
CVE-2024-2873	25-03-2024	wolfSSL Inc.	wolfSSH	9.1		No
CVE-2024-2890	28-03-2024	Tumult Inc.	Tumult Hype Animations	9.1		No
CVE-2024-29100	28-03-2024	Jordy Meow	AI Engine: ChatGPT Chatbot	9.1		No
CVE-2024-30231	26-03-2024	WebToffee	Product Import Export for WooCommerce	9.1		No
CVE-2024-31114	31-03-2024	biplob018	Shortcode Addons	9.1		No
CVE-2023-38388	26-03-2024	Artbees	JupiterX Core	9		No
CVE-2024-30223	28-03-2024	Repute Infosystems	ARMember	9		No
CVE-2024-30226	28-03-2024	WPDeveloper	BetterDocs	9		No
CVE-2024-30227	28-03-2024	INFINITUM FORM	Geo Controller	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