Weekly Vulnerability Report

13 February 2024

This report summarizes the known software vulnerabilities published during the period **5-11 Feb 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 (CISA Known Exploited Catalog).
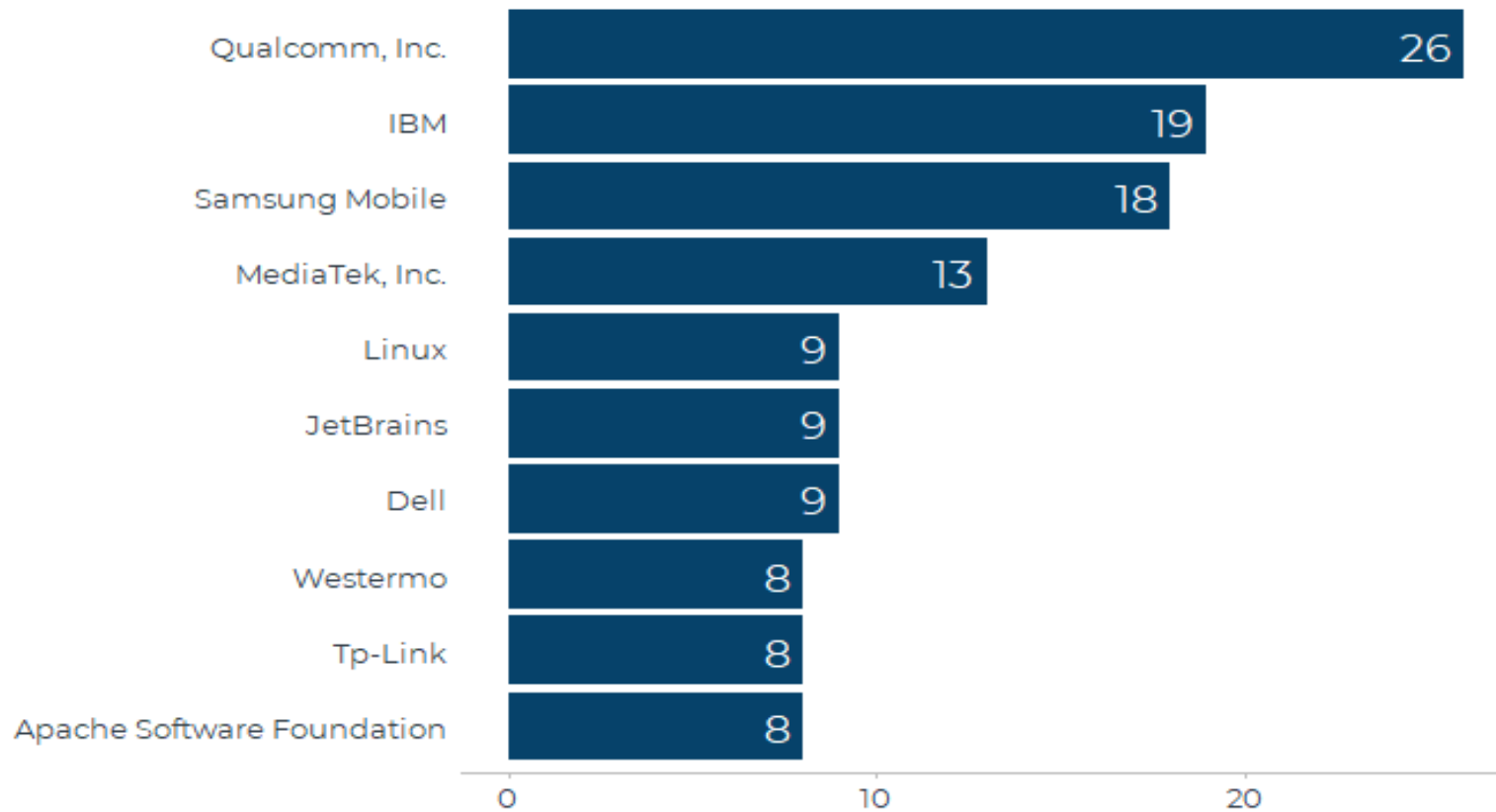
Users can follow the link attached to each CVE number for further information including mitigation or remediation guidance.

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), 5-11 Feb 2024

Vendor	Count
Qualcomm, Inc.	26
IBM	19
Samsung Mobile	18
MediaTek, Inc.	13
Linux	9
JetBrains	9
Dell	9
Westermo	8
Tp-Link	8
Apache Software Foundation	8

Vulnerabilities with highest likelihood of exploitation, 5-11 Feb 2024

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-21762	09-02-2024	Fortinet	FortiProxy	9.6	0.012	Yes
CVE-2023-46359	06-02-2024	Hardy Barth	cPH2 eCharge Ladestation v1.87.0		0.005	No
CVE-2021-4436	05-02-2024	Unknown	3DPrint Lite		0.004	No

Vulnerabilities with highest severity, 5-11 Feb 2024

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-24594	06-02-2024	Allegro.AI	ClearML	9.9		No
CVE-2023-46687	09-02-2024	Emerson	Rosemount GC370XA	9.8		No
CVE-2023-6229	06-02-2024	Canon Inc.	Satera LBP670C Series	9.8	0.001	No
CVE-2023-6230	06-02-2024	Canon Inc.	Satera LBP670C Series	9.8	0.001	No
CVE-2023-6231	06-02-2024	Canon Inc.	Satera LBP670C Series	9.8	0.001	No
CVE-2023-6232	06-02-2024	Canon Inc.	Satera LBP670C Series	9.8	0.001	No
CVE-2023-6233	06-02-2024	Canon Inc.	Satera LBP670C Series	9.8	0.001	No
CVE-2023-6234	06-02-2024	Canon Inc.	Satera LBP670C Series	9.8	0.001	No
CVE-2023-6677	09-02-2024	Oduyo Financial Technology	Online Collection	9.8	0.001	No
CVE-2023-6933	05-02-2024	wpengine	Better Search Replace	9.8	0.001	No
CVE-2023-6989	05-02-2024	paultgoodchild	Shield Security – Smart Bot Blocking & Intrusion Prevention Security	9.8		No
CVE-2024-0244	06-02-2024	Canon Inc.	Satera MF750C Series	9.8	0.001	No

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-0323	05-02-2024	B&R Industrial Automation	Automation Runtime	9.8		No
CVE-2024-0709	05-02-2024	narinder-singh	Cryptocurrency Widgets – Price Ticker & Coins List	9.8		No
CVE-2024-1207	08-02-2024	wpdevelop	WP Booking Calendar	9.8		No
CVE-2024-23917	06-02-2024	JetBrains	TeamCity	9.8	0.001	No
CVE-2024-24563	07-02-2024	vyperlang	vyper	9.8		No
CVE-2024-24592	06-02-2024	Allegro.AI	ClearML	9.8		No
CVE-2024-24811	07-02-2024	zopefoundation	Products.SQLAlchemyDA	9.8		No
CVE-2024-23108	05-02-2024	Fortinet	FortiSIEM	9.7	0.001	No
CVE-2024-23109	05-02-2024	Fortinet	FortiSIEM	9.7	0.001	No
CVE-2024-20252	07-02-2024	Cisco	Cisco TelePresence Video Communication Server (VCS) Expressway	9.6		No
CVE-2024-20254	07-02-2024	Cisco	Cisco TelePresence Video Communication Server (VCS) Expressway	9.6		No

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-21762	09-02-2024	Fortinet	FortiProxy	9.6	0.012	Yes
CVE-2024-24593	06-02-2024	Allegro.AI	ClearML	9.6		No
CVE-2024-25145	07-02-2024	Liferay	Portal	9.6		No
CVE-2023-33072	06-02-2024	Qualcomm, Inc.	Snapdragon	9.3		No
CVE-2024-0221	05-02-2024	10web	Photo Gallery by 10Web – Mobile-Friendly Image Gallery	9.1		No
CVE-2024-24825	08-02-2024	DIRACGrid	DIRAC	9.1		No
CVE-2024-25106	08-02-2024	openobserve	openobserve	9.1		No

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)
· SC3 open-source research

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