Scottish Cyber Coordination Centre

TLP: CLEAR – Disclosure is not limited

Weekly Vulnerability Report

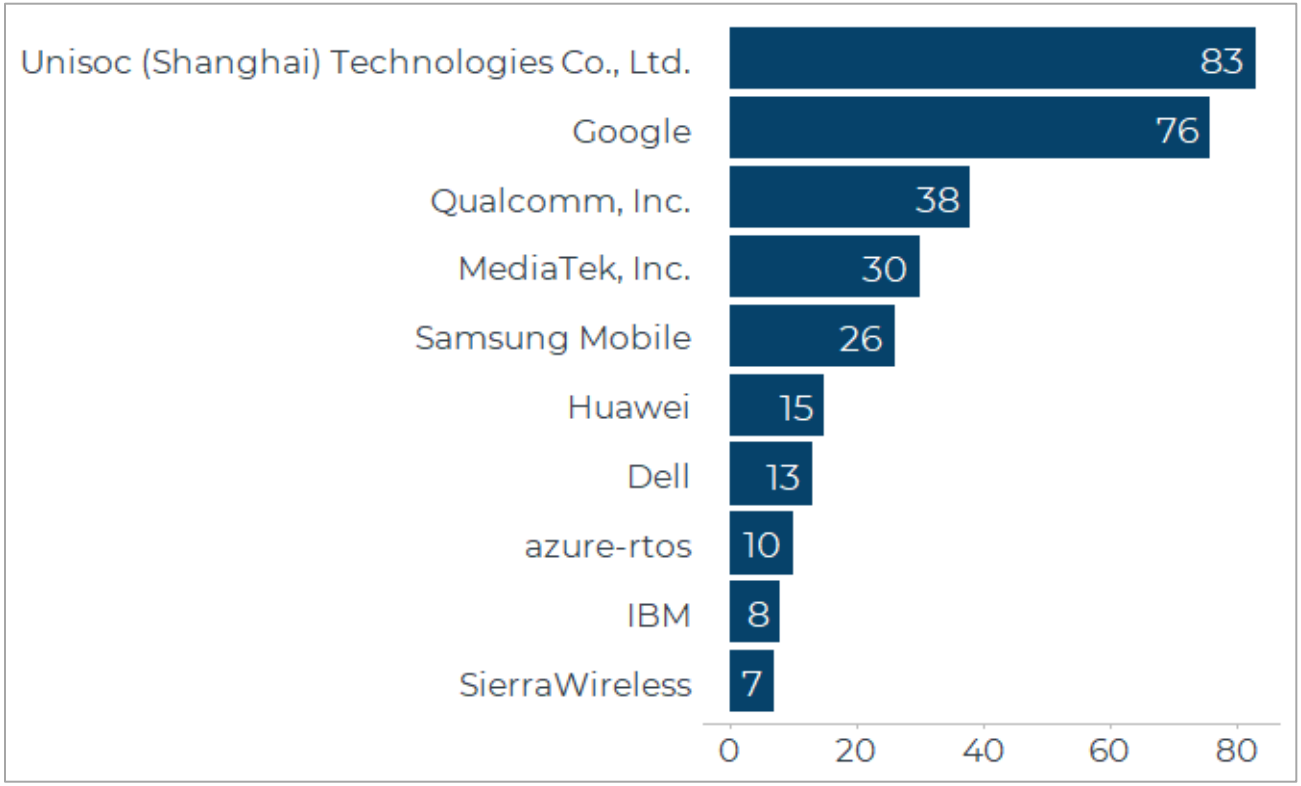
12 December 2023

This report summarizes the known software vulnerabilities published during the period **4-10 December 2023**. 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.

Count of vulnerabilities by software vendor (top 10), 4-10 Dec 2023



Scottish Cyber Coordination Centre

TLP: CLEAR – Disclosure is not limited

Vulnerabilities with highest likelihood of exploitation, 4-10 Dec 2023

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2023-48697	05-12-2023	azure-rtos	usbx	6.4	0.044	No
CVE-2023-48315	05-12-2023	azure-rtos	netxduo	8.8	0.013	No
CVE-2023-48316	05-12-2023	azure-rtos	netxduo	9.8	0.013	No
CVE-2023-48691	05-12-2023	azure-rtos	netxduo	8.1	0.013	No
CVE-2023-48692	05-12-2023	azure-rtos	netxduo	9.1	0.013	No
CVE-2023-48694	05-12-2023	azure-rtos	usbx	6.8	0.013	No
CVE-2023-48695	05-12-2023	azure-rtos	usbx	7.2	0.013	No
CVE-2023-	05-12-2023	azure-rtos	usbx	6.7	0.013	No

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
48696						
CVE-2023-49291	04-12-2023	tj-actions	branch-names	9.3	0.007	No
CVE-2023-5869	10-12-2023	n/a	PostgreSQL		0.004	No
CVE-2023-49285	04-12-2023	squid-cache	squid	8.6	0.004	No
CVE-2023-5868	10-12-2023	n/a	PostgreSQL		0.004	No
CVE-2023-49286	04-12-2023	squid-cache	squid	8.6	0.003	No
CVE-2023-49093	04-12-2023	HtmlUnit	htmlunit	9.8	0.003	No
CVE-2023-48693	05-12-2023	azure-rtos	threadx	8.7	0.003	No
CVE-2023-48823	07-12-2023	n/a	n/a		0.003	No

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2023-48799	04-12-2023	n/a	n/a		0.003	No
CVE-2023-48800	04-12-2023	n/a	n/a		0.003	No
CVE-2023-44302	04-12-2023	Dell	Dell PowerProtect Data Manager DM5500 Appliance	8.1	0.002	No
CVE-2023-49288	04-12-2023	squid-cache	squid	8.6	0.002	No
CVE-2023-41835	05-12-2023	Apache Software Foundation	Apache Struts		0.002	No
CVE-2023-44305	04-12-2023	Dell	Dell PowerProtect Data Manager DM5500 Appliance	8.1	0.002	No
CVE-2023-44304	04-12-2023	Dell	Dell PowerProtect Data Manager DM5500 Appliance	8.8	0.002	No
CVE-2023-49406	07-12-2023	n/a	n/a		0.002	No

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2023-49409	07-12-2023	n/a	n/a		0.002	No
CVE-2023-6063	04-12-2023	Unknown	WP Fastest Cache		0.002	No
CVE-2023-33063	05-12-2023	Qualcomm, Inc.	Snapdragon	7.8	0.002	Yes
CVE-2023-33106	05-12-2023	Qualcomm, Inc.	Snapdragon	8.4	0.002	Yes
CVE-2023-33107	05-12-2023	Qualcomm, Inc.	Snapdragon	8.4	0.002	Yes
CVE-2023-49428	07-12-2023	n/a	n/a		0.002	No
CVE-2023-49431	07-12-2023	n/a	n/a		0.002	No
CVE-2023-49435	07-12-2023	n/a	n/a		0.002	No

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2023-49436	07-12-2023	n/a	n/a		0.002	No
CVE-2023-49437	07-12-2023	n/a	n/a		0.002	No

Scottish Cyber Coordination Centre

TLP: CLEAR – Disclosure is not limited

Vulnerabilities with highest severity, 4-10 Dec 2023

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2023-4122	07-12-2023	Kashipara Group	Student Information System	9.9	0.001	No
CVE-2023-22523	06-12-2023	Atlassian	Assets Discovery Cloud	9.8	0.001	No
CVE-2023-33082	05-12-2023	Qualcomm, Inc.	Snapdragon	9.8		No
CVE-2023-33083	05-12-2023	Qualcomm, Inc.	Snapdragon	9.8		No
CVE-2023-35039	07-12-2023	Be Devious Web Development	Password Reset with Code for WordPress REST API	9.8		No
CVE-2023-39169	07-12-2023	SENEC	Storage Box V1	9.8	0.001	No
CVE-2023-48316	05-12-2023	azure-rtos	netxduo	9.8	0.013	No
CVE-2023-	04-12-2023	HtmlUnit	htmlunit	9.8	0.003	No

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
49093						
CVE-2023-5008	07-12-2023	Kashipara Group	Student Information System	9.8	0.001	No
CVE-2023-5761	07-12-2023	rogierlankhorst	Burst Statistics – Privacy-Friendly Analytics for WordPress	9.8		No
CVE-2023-6448	05-12-2023	Unitronics	Vision Series PLCs and HMIs	9.8		No
CVE-2023-22524	06-12-2023	Atlassian	Companion for Mac	9.6	0.001	No
CVE-2023-35618	07-12-2023	Microsoft	Microsoft Edge (Chromium-based)	9.6	0.001	No
CVE-2023-49291	04-12-2023	tj-actions	branch-names	9.3	0.007	No
CVE-2023-33054	05-12-2023	Qualcomm, Inc.	Snapdragon	9.1		No
CVE-2023-39172	07-12-2023	SENEC	Storage Box V1	9.1		No

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2023-48692	05-12-2023	azure-rtos	netxduo	9.1	0.013	No
CVE-2023-22522	06-12-2023	Atlassian	Confluence Data Center	9	0.001	No

Scottish Cyber Coordination Centre

TLP: CLEAR – Disclosure is not limited

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