Scottish Cyber Coordination Centre

TLP: Clear – Disclosure is not limited

Weekly Vulnerability Report

9 January 2024

This report summarizes the known software vulnerabilities published during the period **1 to 7 January 2024**. This data can help users prioritise and manage the vulnerabilities that might pose a risk to their organisations.

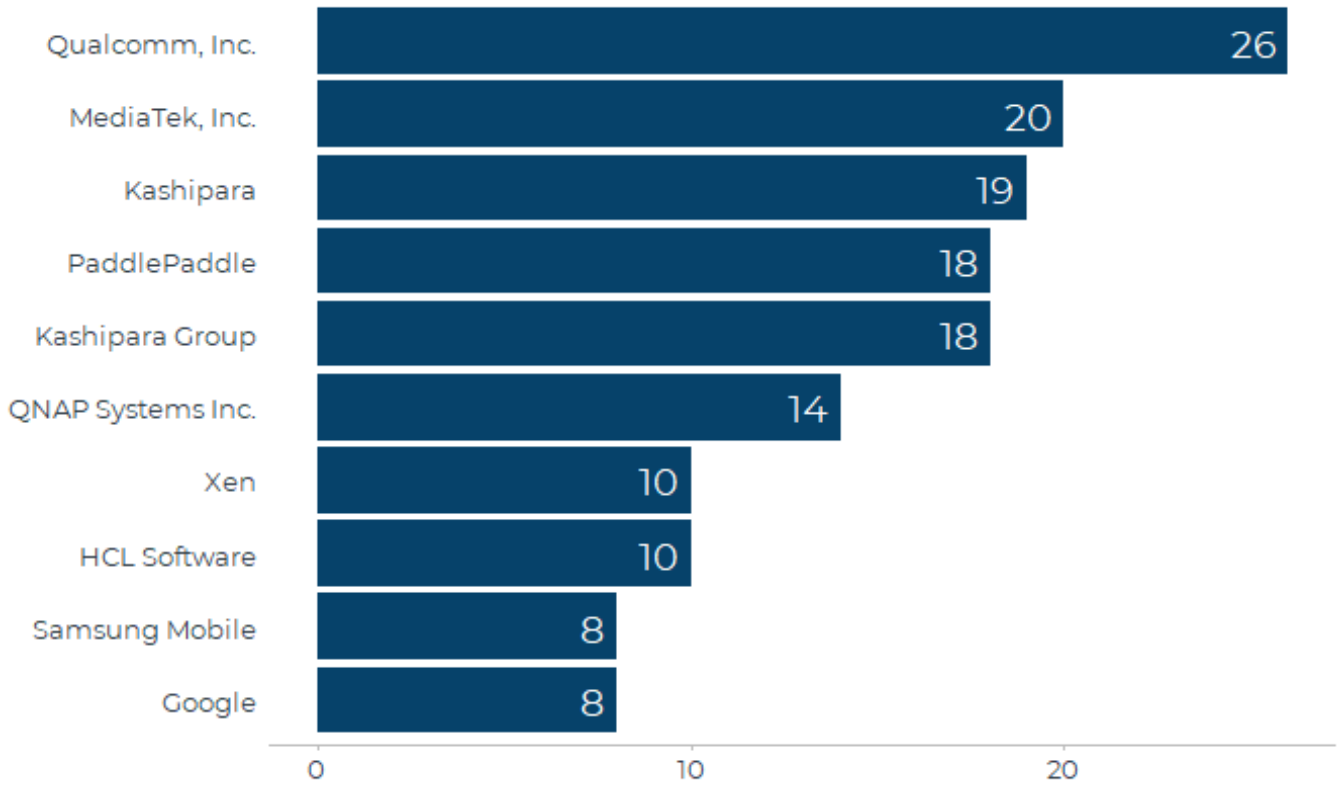
It includes a breakdown of vulnerabilities by vendor, a table of vulnerabilities with the highest likelihood of being exploited (EPSS >0.002), and a table of vulnerabilities with the highest severity rating (CVSSv3 Base Score >=9). The tables also indicate whether a vulnerability has been exploited (CISA Known Exploited Catalog).

Users can follow the link attached to each CVE number for further information including mitigation or remediation guidance.

Scottish Cyber Coordination Centre

TLP: Clear – Disclosure is not limited

Count of vulnerabilities by software vendor (top 10), 1-7 Jan 2024



Scottish Cyber Coordination Centre

TLP: Clear – Disclosure is not limited

Vulnerabilities with highest likelihood of exploitation, 1-7 Jan 2024

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2023-32874	02-01-2024	MediaTek, Inc.	Modem IMS Stack		0.002	No

Scottish Cyber Coordination Centre

TLP: Clear – Disclosure is not limited

Vulnerabilities with highest severity, 1-7 Jan 2024

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2023-33025	02-01-2024	Qualcomm, Inc.	Snapdragon	9.8	0.001	No
CVE-2023-49622	04-01-2024	Kashipara Group	Billing Software	9.8		No
CVE-2023-49624	04-01-2024	Kashipara Group	Billing Software	9.8		No
CVE-2023-49625	04-01-2024	Kashipara Group	Billing Software	9.8		No
CVE-2023-49633	04-01-2024	Kashipara Group	Billing Software	9.8		No
CVE-2023-49639	04-01-2024	Kashipara Group	Billing Software	9.8		No
CVE-2023-49658	04-01-2024	Kashipara Group	Billing Software	9.8		No
CVE-2023-49665	04-01-2024	Kashipara Group	Billing Software	9.8		No

Scottish Cyber Coordination Centre

TLP: Clear – Disclosure is not limited

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2023-49666	04-01-2024	Kashipara Group	Billing Software	9.8		No
CVE-2023-50743	04-01-2024	Kashipara Group	Online Notice Board System	9.8		No
CVE-2023-50752	04-01-2024	Kashipara Group	Online Notice Board System	9.8		No
CVE-2023-50753	04-01-2024	Kashipara Group	Online Notice Board System	9.8		No
CVE-2023-50862	04-01-2024	Kashipara Group	Travel Website	9.8		No
CVE-2023-50863	04-01-2024	Kashipara Group	Travel Website	9.8		No
CVE-2023-50864	04-01-2024	Kashipara Group	Travel Website	9.8		No
CVE-2023-50865	04-01-2024	Kashipara Group	Travel Website	9.8		No
CVE-2023-50866	04-01-2024	Kashipara Group	Travel Website	9.8		No

Scottish Cyber Coordination Centre

TLP: Clear – Disclosure is not limited

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2023-50867	04-01-2024	Kashipara Group	Travel Website	9.8		No
CVE-2023-6436	02-01-2024	Ekol Informatics	Website Template	9.8		No
CVE-2024-21623	02-01-2024	mehah	otclient	9.8		No
CVE-2023-50253	03-01-2024	labring	laf	9.7		No
CVE-2023-52310	03-01-2024	PaddlePaddle	PaddlePaddle	9.6		No
CVE-2023-52311	03-01-2024	PaddlePaddle	PaddlePaddle	9.6		No
CVE-2023-52314	03-01-2024	PaddlePaddle	PaddlePaddle	9.6		No
CVE-2023-33030	02-01-2024	Qualcomm, Inc.	Snapdragon	9.3	0.001	No
CVE-2023-33032	02-01-2024	Qualcomm, Inc.	Snapdragon	9.3	0.001	No

Scottish Cyber Coordination Centre

TLP: Clear – Disclosure is not limited

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2023-4280	02-01-2024	silabs.com	GSDK	9.3		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