Scottish Cyber Coordination Centre

Weekly Vulnerability Report

9 July 2024

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

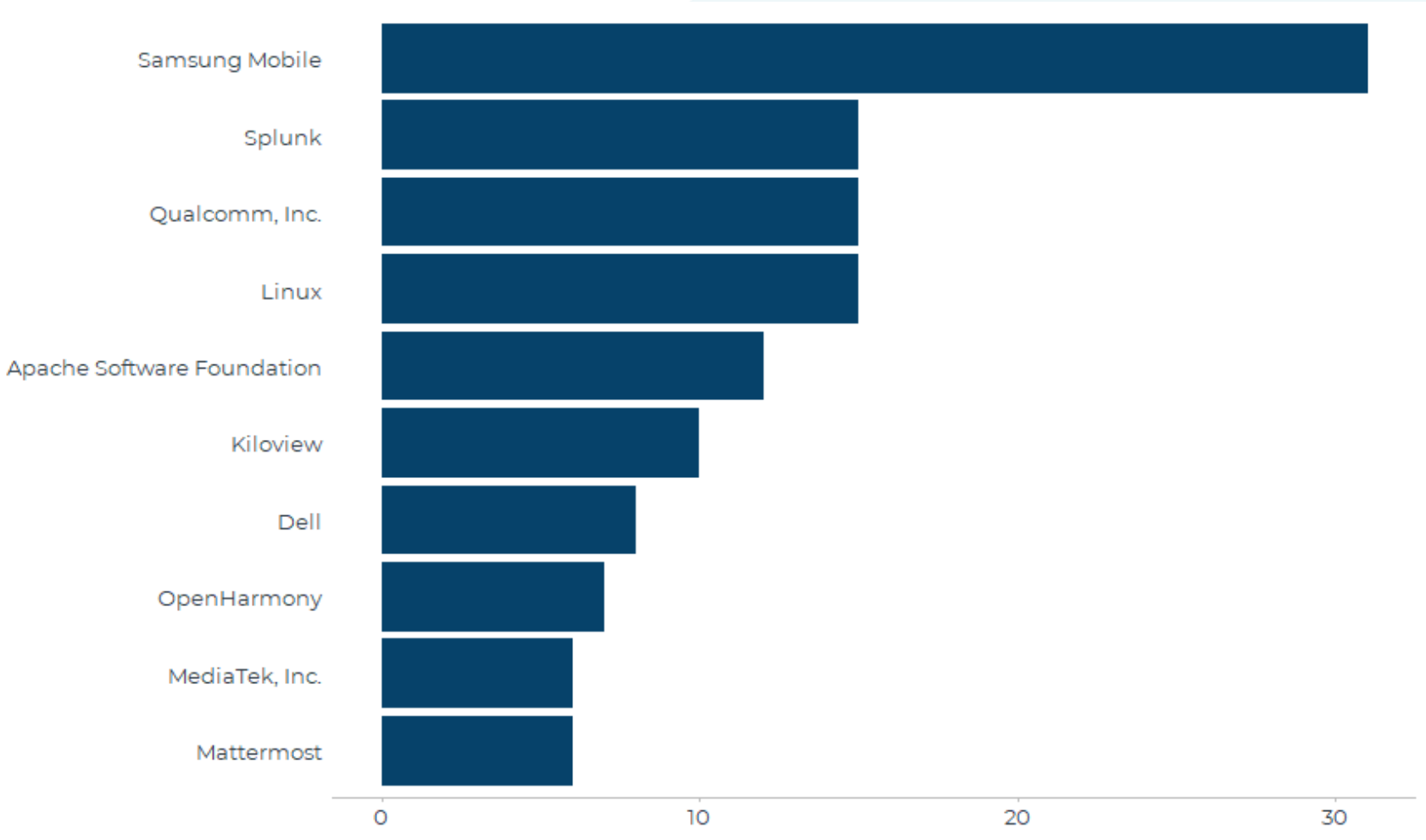
It includes a breakdown of vulnerabilities by vendor, a table of vulnerabilities with the highest likelihood of being exploited (EPSS >0.001), and a table of vulnerabilities with the highest severity rating (CVSSv3 Base Score >=9). The tables also indicate whether a vulnerability has been exploited according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

Scottish Cyber Coordination Centre

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



Scottish Cyber Coordination Centre

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

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-36401	01-07-2024	geoserver	geoserver	9.8	0.177	No
CVE-2024-6387	01-07-2024	Red Hat	Red Hat Enterprise Linux 9	NA	0.049	No
CVE-2024-6439	02-07-2024	SourceCodester	Home Owners Collection Management System	5.3	0.003	No
CVE-2024-20399	01-07-2024	Cisco	Cisco NX-OS Software	6	0.003	Yes
CVE-2024-6438	02-07-2024	Hitout	Carsale	5.3	0.002	No
CVE-2024-6440	02-07-2024	SourceCodester	Home Owners Collection Management System	5.3	0.001	No

Scottish Cyber Coordination Centre

Vulnerabilities with highest severity, 1-7 July 2024

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-39930	04-07-2024	n/a	n/a	9.9		No
CVE-2024-39931	04-07-2024	n/a	n/a	9.9		No
CVE-2024-39932	04-07-2024	n/a	n/a	9.9		No
CVE-2024-39943	04-07-2024	n/a	n/a	9.9		No
CVE-2023-41919	02-07-2024	Kiloview	P1/P2	9.8		No
CVE-2023-41920	02-07-2024	Kiloview	P1/P2	9.8		No
CVE-2023-41921	02-07-2024	Kiloview	P1/P2	9.8		No
CVE-2024-20078	01-07-2024	MediaTek, Inc.	MT6768, MT6779, MT8321, MT8385, MT8755, MT8765, MT8766, MT8768, MT8771, MT8775, MT8781, MT8786, MT8788, MT8789, MT8791T, MT8792, MT8795T, MT8796, MT8797, MT8798	9.8		No
CVE-2024-36401	01-07-2024	geoserver	geoserver	9.8	0.177	No

Scottish Cyber Coordination Centre

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-36404	02-07-2024	geotools	geotools	9.8		No
CVE-2024-38993	01-07-2024	n/a	n/a	9.8		No
CVE-2024-38996	01-07-2024	n/a	n/a	9.8		No
CVE-2024-39015	01-07-2024	n/a	n/a	9.8		No
CVE-2024-39017	01-07-2024	n/a	n/a	9.8		No
CVE-2024-39236	01-07-2024	n/a	n/a	9.8		No
CVE-2024-39309	01-07-2024	parse-community	parse-server	9.8		No
CVE-2024-39844	03-07-2024	n/a	n/a	9.8		No
CVE-2024-6172	02-07-2024	icegram	Email Subscribers by Icegram Express – Email Marketing, Newsletters, Automation for WordPress & WooCommerce	9.8	0.001	No
CVE-2024-6209	05-07-2024	ABB	ASPECT-Enterprise	9.4		No

Scottish Cyber Coordination Centre

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-6298	05-07-2024	ABB	ASPECT-Enterprise	9.4		No
CVE-2024-38368	01-07-2024	CocoaPods	CocoaPods	9.3		No
CVE-2024-4708	02-07-2024	mySCADA	myPRO	9.3		No
CVE-2024-6424	01-07-2024	MESbook	MESbook	9.3		No
CVE-2024-28200	01-07-2024	N-able	N-central	9.1		No
CVE-2024-32755	02-07-2024	Johnson Controls	American Dynamics Illustra Essentials Gen 4	9.1		No
CVE-2024-38475	01-07-2024	Apache Software Foundation	Apache HTTP Server	9.1		No
CVE-2024-5322	01-07-2024	N-able	N-central	9.1		No
CVE-2024-6425	01-07-2024	MESbook	MESbook	9.1		No
CVE-2024-37082	03-07-2024	Routing Release	Routing Release	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