



Scottish
Cyber
Coordination
Centre

Weekly Vulnerability Report

13 August 2024

This report summarizes the known software vulnerabilities published during the period **5-11 August 2024**. This data can help users prioritise and manage the vulnerabilities that might pose a risk to their organisations.

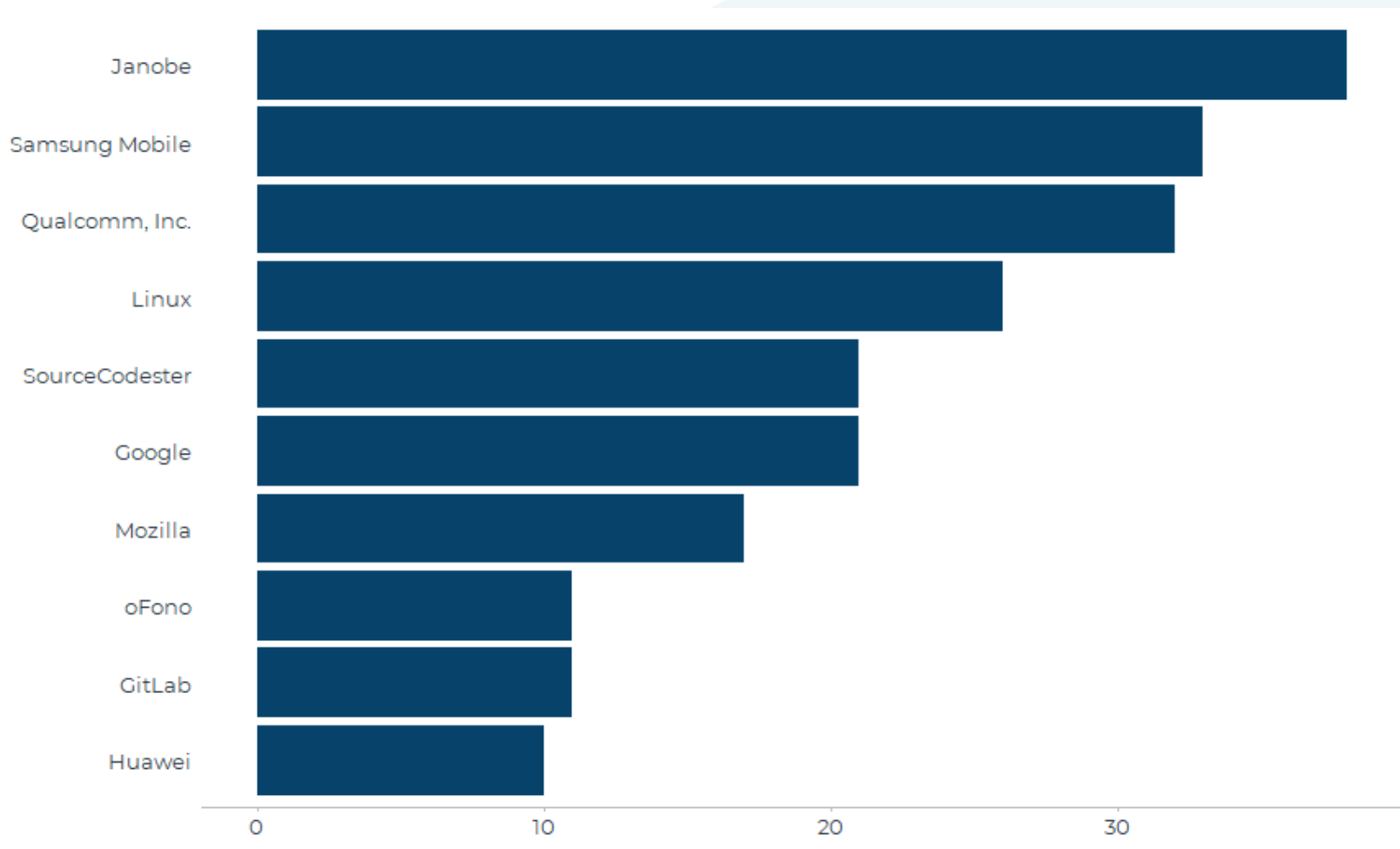
It includes a breakdown of vulnerabilities by vendor, a table of vulnerabilities with the highest likelihood of being exploited ([EPSS >0.001](#)), and a table of vulnerabilities with the highest severity rating ([CVSSv3 Base Score >=9](#)). The tables also indicate whether a vulnerability has been exploited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



Count of vulnerabilities by software vendor (top 10), 5-11 August 2024





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

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-7467	05-08-2024	Raisecom	MSG1200	5.3	0.017	No
CVE-2024-7468	05-08-2024	Raisecom	MSG1200	5.3	0.017	No
CVE-2024-7469	05-08-2024	Raisecom	MSG1200	5.3	0.017	No
CVE-2024-7470	05-08-2024	Raisecom	MSG1200	5.3	0.017	No
CVE-2024-6782	06-08-2024	Calibre	Calibre	9.8	0.002	No



Vulnerabilities with highest severity, 5-11 August 2024

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-22116	09-08-2024	Zabbix	Zabbix	9.9	NA	No
CVE-2024-20450	07-08-2024	Cisco	Cisco Small Business IP Phones	9.8	NA	No
CVE-2024-20454	07-08-2024	Cisco	Cisco Small Business IP Phones	9.8	NA	No
CVE-2024-33957	06-08-2024	Janobe	E-Negosyo System	9.8	NA	No
CVE-2024-33958	06-08-2024	Janobe	E-Negosyo System	9.8	NA	No
CVE-2024-33959	06-08-2024	Janobe	Janobe PayPal	9.8	NA	No
CVE-2024-33960	06-08-2024	Janobe	Janobe PayPal	9.8	NA	No
CVE-2024-33961	06-08-2024	Janobe	Janobe PayPal	9.8	NA	No
CVE-2024-33962	06-08-2024	Janobe	Janobe PayPal	9.8	NA	No
CVE-2024-33963	06-08-2024	Janobe	Janobe PayPal	9.8	NA	No
CVE-2024-33964	06-08-2024	Janobe	Janobe PayPal	9.8	NA	No



CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-33965	06-08-2024	Janobe	Janobe PayPal	9.8	NA	No
CVE-2024-33966	06-08-2024	Janobe	Janobe PayPal	9.8	NA	No
CVE-2024-33967	06-08-2024	Janobe	School Attendance Monitoring System	9.8	NA	No
CVE-2024-33968	06-08-2024	Janobe	School Attendance Monitoring System	9.8	NA	No
CVE-2024-33969	06-08-2024	Janobe	School Attendance Monitoring System	9.8	NA	No
CVE-2024-33970	06-08-2024	Janobe	School Attendance Monitoring System	9.8	NA	No
CVE-2024-33971	06-08-2024	Janobe	School Attendance Monitoring System	9.8	NA	No
CVE-2024-33972	06-08-2024	Janobe	School Attendance Monitoring System	9.8	NA	No
CVE-2024-33973	06-08-2024	Janobe	School Attendance Monitoring System	9.8	NA	No
CVE-2024-33974	06-08-2024	Janobe	School Attendance Monitoring System	9.8	NA	No
CVE-2024-34479	07-08-2024	n/a	n/a	9.8	NA	No
CVE-2024-34480	07-08-2024	n/a	n/a	9.8	NA	No



CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-36130	07-08-2024	Ivanti	EPMM	9.8	NA	No
CVE-2024-39225	06-08-2024	n/a	n/a	9.8	NA	No
CVE-2024-39228	06-08-2024	n/a	n/a	9.8	NA	No
CVE-2024-40477	08-08-2024	n/a	n/a	9.8	NA	No
CVE-2024-40482	08-08-2024	n/a	n/a	9.8	NA	No
CVE-2024-40486	08-08-2024	n/a	n/a	9.8	NA	No
CVE-2024-40498	05-08-2024	n/a	n/a	9.8		No
CVE-2024-40530	05-08-2024	n/a	n/a	9.8		No
CVE-2024-41237	07-08-2024	n/a	n/a	9.8	NA	No
CVE-2024-41476	09-08-2024	n/a	n/a	9.8	NA	No
CVE-2024-41570	09-08-2024	n/a	n/a	9.8	NA	No
CVE-2024-42393	06-08-2024	Hewlett Packard Enterprise (HPE)	Hpe Aruba Networking InstantOS and Aruba	9.8	NA	No



CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
			Access Points running ArubaOS 10			
CVE-2024-42394	06-08-2024	Hewlett Packard Enterprise (HPE)	HPE Aruba Networking InstantOS and Aruba Access Points running ArubaOS 10	9.8	NA	No
CVE-2024-42395	06-08-2024	Hewlett Packard Enterprise (HPE)	HPE Aruba Networking InstantOS and Aruba Access Points running ArubaOS 10	9.8	NA	No
CVE-2024-42469	09-08-2024	openhab	openhab-webui	9.8	NA	No
CVE-2024-6202	06-08-2024	Halo Service Solutions	HaloITSM	9.8	NA	No
CVE-2024-6782	06-08-2024	Calibre	Calibre	9.8	0.002	No
CVE-2024-6890	07-08-2024	Journyx	Journyx (jtime)	9.8	NA	No
CVE-2024-6995	06-08-2024	Google	Chrome	9.8	NA	No
CVE-2024-7350	08-08-2024	reputeinfosystems	Appointment Booking Calendar Plugin and Scheduling Plugin – BookingPress	9.8	NA	No
CVE-2024-7521	06-08-2024	Mozilla	Firefox	9.8	NA	No



CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-7528	06-08-2024	Mozilla	Firefox	9.8	NA	No
CVE-2024-7530	06-08-2024	Mozilla	Firefox	9.8	NA	No
CVE-2024-28739	06-08-2024	n/a	n/a	9.6	NA	No
CVE-2024-7490	08-08-2024	Microchip Technology	Advanced Software Framework	9.5	NA	No
CVE-2024-21876	10-08-2024	Enphase	IQ Gateway	9.3	NA	No
CVE-2024-42037	08-08-2024	Huawei	HarmonyOS	9.3	NA	No
CVE-2024-6117	05-08-2024	Hamastar Technology	MeetingHub Paperless Meetings	9.3		No
CVE-2024-6118	05-08-2024	Hamastar Technology	MeetingHub Paperless Meetings	9.3		No
CVE-2024-6915	05-08-2024	JFrog	Artifactory	9.3		No
CVE-2024-7395	05-08-2024	Korenix	JetPort 5601v3	9.3		No
CVE-2024-7397	05-08-2024	Korenix	JetPort 5601v3	9.3		No
CVE-2024-3279	09-08-2024	mintplex-labs	mintplex-labs/anything-llm	9.1	NA	No



CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-36461	09-08-2024	Zabbix	Zabbix	9.1	NA	No
CVE-2024-37023	08-08-2024	Vonets	VAR1200-H	9.1	NA	No
CVE-2024-39815	08-08-2024	Vonets	VAR1200-H	9.1	NA	No
CVE-2024-41247	07-08-2024	n/a	n/a	9.1	NA	No
CVE-2024-42366	08-08-2024	vrcx-team	VRCX	9.1	NA	No
CVE-2024-7522	06-08-2024	Mozilla	Firefox	9.1	NA	No
CVE-2024-7525	06-08-2024	Mozilla	Firefox	9.1	NA	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