Scottish Cyber Coordination Centre

Weekly Vulnerability Report

26 November 2024

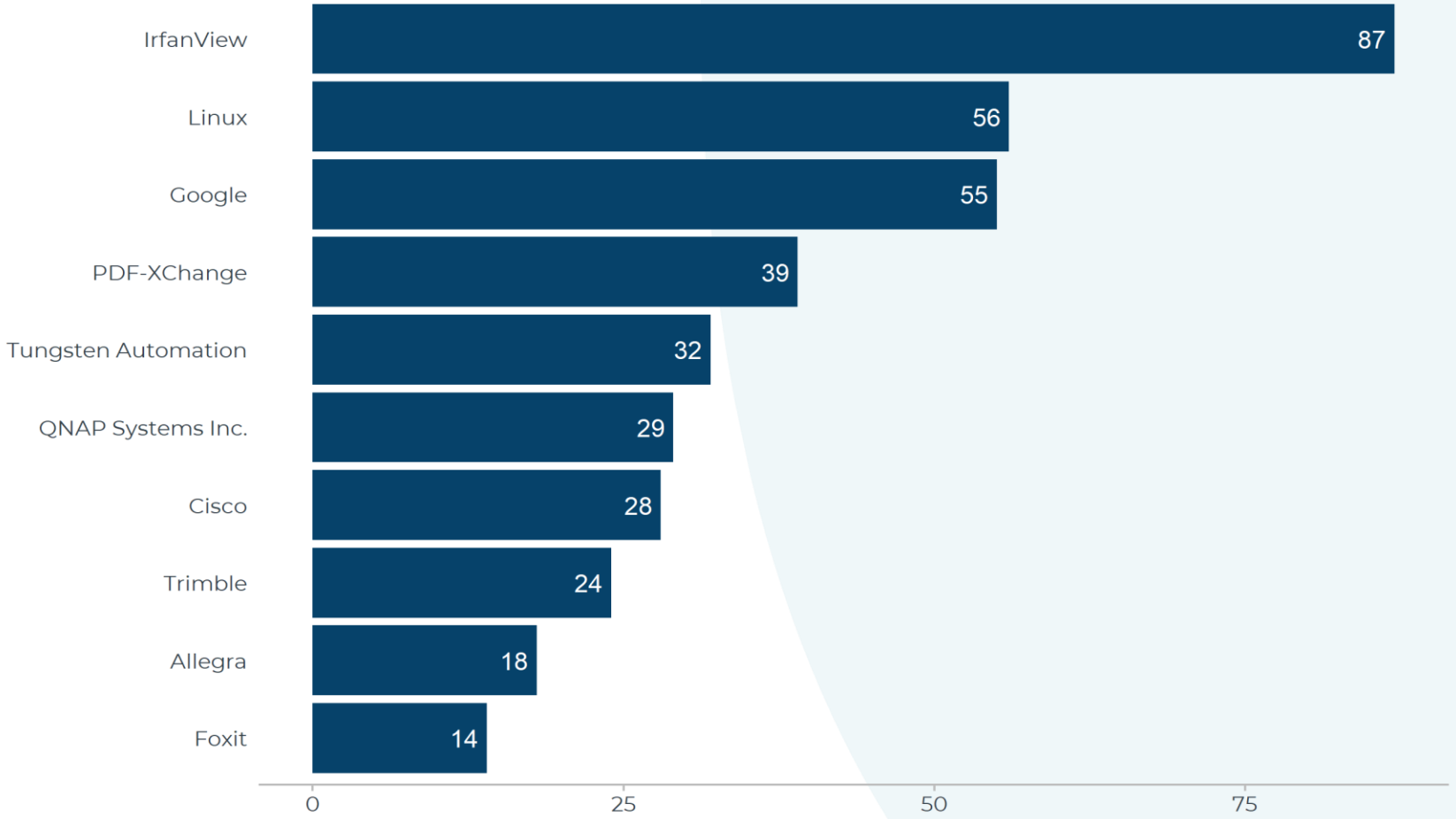
This report summarizes the known software vulnerabilities published during the period **18-24 November 2024**. This data can help users prioritise and manage the vulnerabilities that might pose a risk to their organisations.

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.

Scottish Cyber Coordination Centre

Count of vulnerabilities by software vendor (top 10), 18-24 November 2024



Scottish Cyber Coordination Centre

Vulnerabilities with highest likelihood of exploitation, 18-24 November 2024

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-9474	18-11-2024	Palo Alto Networks	Cloud NGFW	6.9	0.974	Yes
CVE-2024-0012	18-11-2024	Palo Alto Networks	Cloud NGFW	9.3	0.966	Yes
CVE-2020-26073	18-11-2024	Cisco	Cisco Catalyst SD-WAN Manager	7.5	0.007	No
CVE-2024-44308	19-11-2024	Apple	Safari	8.8	0.002	Yes
CVE-2024-44309	19-11-2024	Apple	Safari	6.3	0.002	Yes
CVE-2024-52433	18-11-2024	Mindstien Technologies	My Geo Posts Free	9.8	0.001	No

Scottish Cyber Coordination Centre

Vulnerabilities with highest severity, 18-24 November 2024

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-52427	18-11-2024	Saso Nikolov	Event Tickets with Ticket Scanner	9.9		No
CVE-2024-52429	18-11-2024	Anton Hoelstad	WP Quick Setup	9.9		No
CVE-2018-9341	19-11-2024	Google	Android	9.8		No
CVE-2018-9365	19-11-2024	Google	Andrioid	9.8		No
CVE-2018-9433	19-11-2024	Google	Android	9.8		No
CVE-2018-9467	19-11-2024	Google	Android	9.8		No
CVE-2018-9471	20-11-2024	Google	Android	9.8		No
CVE-2018-9478	20-11-2024	Google	Android	9.8		No
CVE-2018-9479	20-11-2024	Google	Android	9.8		No
CVE-2023-51638	22-11-2024	Allegra	Allegra	9.8		No
CVE-2023-51639	22-11-2024	Allegra	Allegra	9.8		No

Scottish Cyber Coordination Centre

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2023-51641	22-11-2024	Allegra	Allegra	9.8		No
CVE-2023-51642	22-11-2024	Allegra	Allegra	9.8		No
CVE-2023-51644	22-11-2024	Allegra	Allegra	9.8		No
CVE-2023-52333	22-11-2024	Allegra	Allegra	9.8		No
CVE-2024-0138	22-11-2024	NVIDIA	Base Command Manager	9.8		No
CVE-2024-10961	23-11-2024	claudeschlesser	Social Login	9.8		No
CVE-2024-11236	24-11-2024	PHP Group	PHP	9.8		No
CVE-2024-11311	18-11-2024	TRCore	DVC	9.8	0.001	No
CVE-2024-11312	18-11-2024	TRCore	DVC	9.8	0.001	No
CVE-2024-11313	18-11-2024	TRCore	DVC	9.8	0.001	No
CVE-2024-11314	18-11-2024	TRCore	DVC	9.8	0.001	No
CVE-2024-11315	18-11-2024	TRCore	DVC	9.8	0.001	No

Scottish Cyber Coordination Centre

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-21855	21-11-2024	GoCast	GoCast	9.8		No
CVE-2024-28892	21-11-2024	GoCast	GoCast	9.8		No
CVE-2024-29224	21-11-2024	GoCast	GoCast	9.8		No
CVE-2024-41779	22-11-2024	IBM	Engineering Systems Design Rhapsody - Model Manager	9.8		No
CVE-2024-47138	22-11-2024	mySCADA	myPRO Manager	9.8		No
CVE-2024-47208	18-11-2024	Apache Software Foundation	Apache OFBiz	9.8	0.001	No
CVE-2024-47533	18-11-2024	cobbler	cobbler	9.8		No
CVE-2024-52316	18-11-2024	Apache Software Foundation	Apache Tomcat	9.8		No
CVE-2024-52430	18-11-2024	Lis	Lis Video Gallery	9.8	0.001	No
CVE-2024-52432	18-11-2024	NIX Solutions Ltd	NIX Anti-Spam Light	9.8	0.001	No
CVE-2024-52433	18-11-2024	Mindstien Technologies	My Geo Posts Free	9.8	0.001	No

Scottish Cyber Coordination Centre

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-52439	20-11-2024	Mark O'Donnell	Team Rosters	9.8		No
CVE-2024-52440	20-11-2024	Bueno Labs Pvt. Ltd.	Xpresslane Fast Checkout	9.8		No
CVE-2024-52441	20-11-2024	Rajesh Thanoch	Quick Learn	9.8		No
CVE-2024-52442	20-11-2024	Userplus	UserPlus	9.8		No
CVE-2024-52443	20-11-2024	Nerijus Masikonis	Geolocator	9.8		No
CVE-2024-8806	22-11-2024	Cohesive Networks	VNS3	9.8		No
CVE-2024-8807	22-11-2024	Cohesive Networks	VNS3	9.8		No
CVE-2024-8932	22-11-2024	PHP Group	PHP	9.8		No
CVE-2024-9511	23-11-2024	techjewel	FluentSMTP – WP SMTP Plugin with Amazon SES, SendGrid, MailGun, Postmark, Google and Any SMTP Provider	9.8		No
CVE-2024-9659	23-11-2024	dasinfomedia	School Management System for Wordpress	9.8		No
CVE-2024-9942	23-11-2024	dasinfomedia	WPGYM - Wordpress Gym Management System	9.8		No

Scottish Cyber Coordination Centre

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-52401	19-11-2024	荒野无灯	Hacklog DownloadManager	9.6		No
CVE-2024-52402	19-11-2024	Cliconomics	Exclusive Content Password Protect	9.6		No
CVE-2024-6246	22-11-2024	Wyze	Cam v3	9.6	0.001	No
CVE-2024-48860	22-11-2024	QNAP Systems Inc.	QuRouter	9.5		No
CVE-2024-38645	22-11-2024	QNAP Systems Inc.	Notes Station 3	9.4		No
CVE-2024-52052	21-11-2024	Wowza	Streaming Engine	9.4		No
CVE-2024-0012	18-11-2024	Palo Alto Networks	Cloud NGFW	9.3	0.966	Yes
CVE-2024-38643	22-11-2024	QNAP Systems Inc.	Notes Station 3	9.3		No
CVE-2024-52431	18-11-2024	Pressaholic	WordPress Video Robot - The Ultimate Video Importer	9.3	0.001	No
CVE-2024-10127	20-11-2024	M-Files Corporation	M-Files Server	9.2		No
CVE-2024-10094	20-11-2024	Pegasystems	Pega Infinity	9.1		No
CVE-2024-52434	18-11-2024	Supsystic	Popup by Supsystic	9.1		No

Scottish Cyber Coordination Centre

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-11666	24-11-2024	hardy-barth	cph2_echarge_firmware	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