



Scottish
Cyber
Coordination
Centre

Weekly Vulnerability Report

17 December 2024

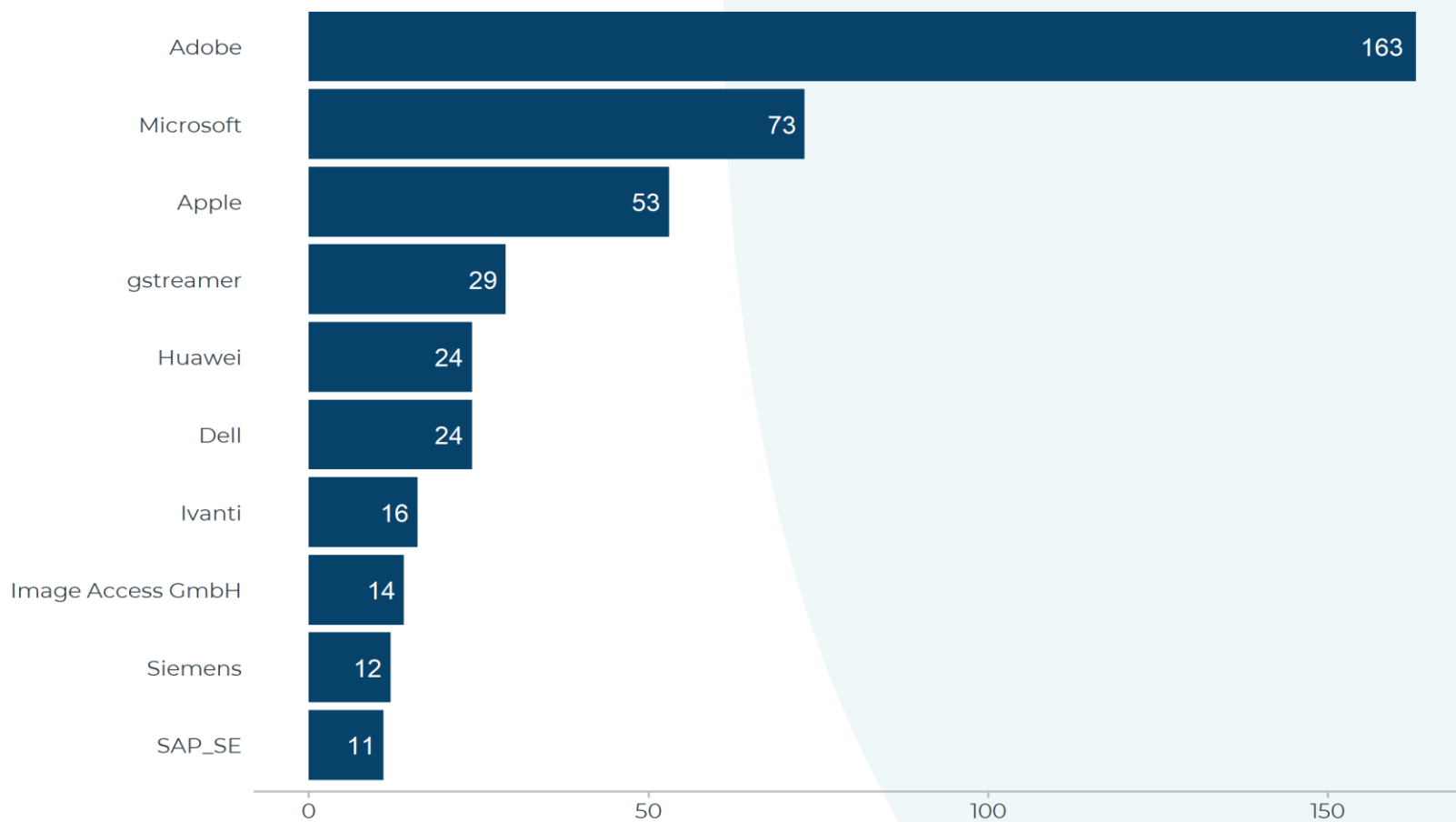
This report summarizes the known software vulnerabilities published during the period **9-15 December 2024**. This data can help users prioritise and manage the vulnerabilities that might pose a risk to their organisations.

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.



Count of vulnerabilities by software vendor (top 10), 9-15 December 2024





Scottish
Cyber
Coordination
Centre

Vulnerabilities with highest likelihood of exploitation, 9-15 December 2024

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-49138	10-12-2024	Microsoft	Windows 10 Version 1809	7.8	0.002	Yes



Vulnerabilities with highest severity, 9-15 December 2024

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-42448	11-12-2024	Veeam	Service Provider Console	9.9		No
CVE-2024-54262	13-12-2024	Siddharth Nagar	Import Export For WooCommerce	9.9		No
CVE-2023-32117	09-12-2024	SoftLab	Integrate Google Drive	9.8	0.001	No
CVE-2024-10124	12-12-2024	themehunk	Vayu Blocks – Gutenberg Blocks for WordPress & WooCommerce	9.8		No
CVE-2024-11015	12-12-2024	tarecord	Sign In With Google	9.8		No
CVE-2024-11948	11-12-2024	GFI	Archiver	9.8		No
CVE-2024-43222	09-12-2024	Envato Security Team	Sweet Date	9.8		No
CVE-2024-44241	11-12-2024	Apple	iOS and iPadOS	9.8		No
CVE-2024-44242	11-12-2024	Apple	iOS and iPadOS	9.8		No
CVE-2024-49112	10-12-2024	Microsoft	Windows 10 Version 1809	9.8		No



CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-54239	13-12-2024	dugudlabs	Eyewear prescription form	9.8		No
CVE-2024-54273	13-12-2024	PickPlugins	Mail Picker	9.8		No
CVE-2024-54293	13-12-2024	CE2I	CE2I Suite	9.8		No
CVE-2024-54294	13-12-2024	appgenixinfotech	Firebase OTP Authentication	9.8		No
CVE-2024-54295	13-12-2024	InspireUI	ListApp Mobile Manager	9.8		No
CVE-2024-54296	13-12-2024	Codexpert, Inc	CoSchool LMS	9.8		No
CVE-2024-54297	13-12-2024	www.vbssso.com	vBSSO-lite	9.8		No
CVE-2024-54492	11-12-2024	Apple	visionOS	9.8		No
CVE-2024-55636	09-12-2024	Drupal	Drupal Core	9.8		No
CVE-2024-55637	09-12-2024	Drupal	Drupal Core	9.8		No
CVE-2024-55638	09-12-2024	Drupal	Drupal Core	9.8		No
CVE-2024-55875	12-12-2024	http4k	http4k	9.8		No



CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-5660	10-12-2024	Arm	Cortex-A77	9.8		No
CVE-2024-8259	09-12-2024	Eryaz Information Technologies	NatraCar B2B Dealer Management Program	9.8		No
CVE-2024-9290	13-12-2024	azzaroco	Super Backup & Clone - Migrate for WordPress	9.8		No
CVE-2024-11986	13-12-2024	CrushFTP, LLC	CrushFTP	9.6		No
CVE-2024-53677	11-12-2024	Apache Software Foundation	Apache Struts	9.5		No
CVE-2024-11737	11-12-2024	Schneider Electric	Modicon Controllers M241 / M251	9.3		No
CVE-2024-12286	10-12-2024	MOBATIME	Network Master Clock - DTS 4801	9.3		No
CVE-2024-49147	12-12-2024	Microsoft	Microsoft Update Catalog	9.3		No
CVE-2024-50339	11-12-2024	glpi-project	glpi	9.3		No
CVE-2024-54032	10-12-2024	Adobe	Adobe Connect	9.3		No
CVE-2024-54152	10-12-2024	peerigon	angular-expressions	9.3		No
CVE-2024-54215	09-12-2024	Roninwp	Revy	9.3		No



CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-54234	13-12-2024	wp-buy	Limit Login Attempts	9.3		No
CVE-2024-54292	13-12-2024	Appsplate	Appsplate	9.3		No
CVE-2024-55547	10-12-2024	ORing	IAP-420	9.3		No
CVE-2022-46838	13-12-2024	JS Help Desk	JS Help Desk – Best Help Desk & Support Plugin	9.1		No
CVE-2024-11633	10-12-2024	Ivanti	Connect Secure	9.1		No
CVE-2024-11634	10-12-2024	Ivanti	Connect Secure	9.1		No
CVE-2024-11772	10-12-2024	Ivanti	Cloud Services Application	9.1		No
CVE-2024-11773	10-12-2024	Ivanti	Cloud Services Application	9.1		No
CVE-2024-45337	11-12-2024	golang.org/x/crypto	golang.org/x/crypto/ssh	9.1		No
CVE-2024-47578	10-12-2024	SAP_SE	SAP NetWeaver AS for JAVA (Adobe Document Services)	9.1		No
CVE-2024-52057	13-12-2024	RTI	Connex Professional	9.1		No
CVE-2024-55879	12-12-2024	xwiki	xwiki-platform	9.1		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