



Scottish  
Cyber  
Coordination  
Centre

TLP: Clear – Disclosure is not limited.

# Weekly Vulnerability Report

16 January 2024

This report summarizes the known software vulnerabilities published during the period **8 to 14 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](#)).

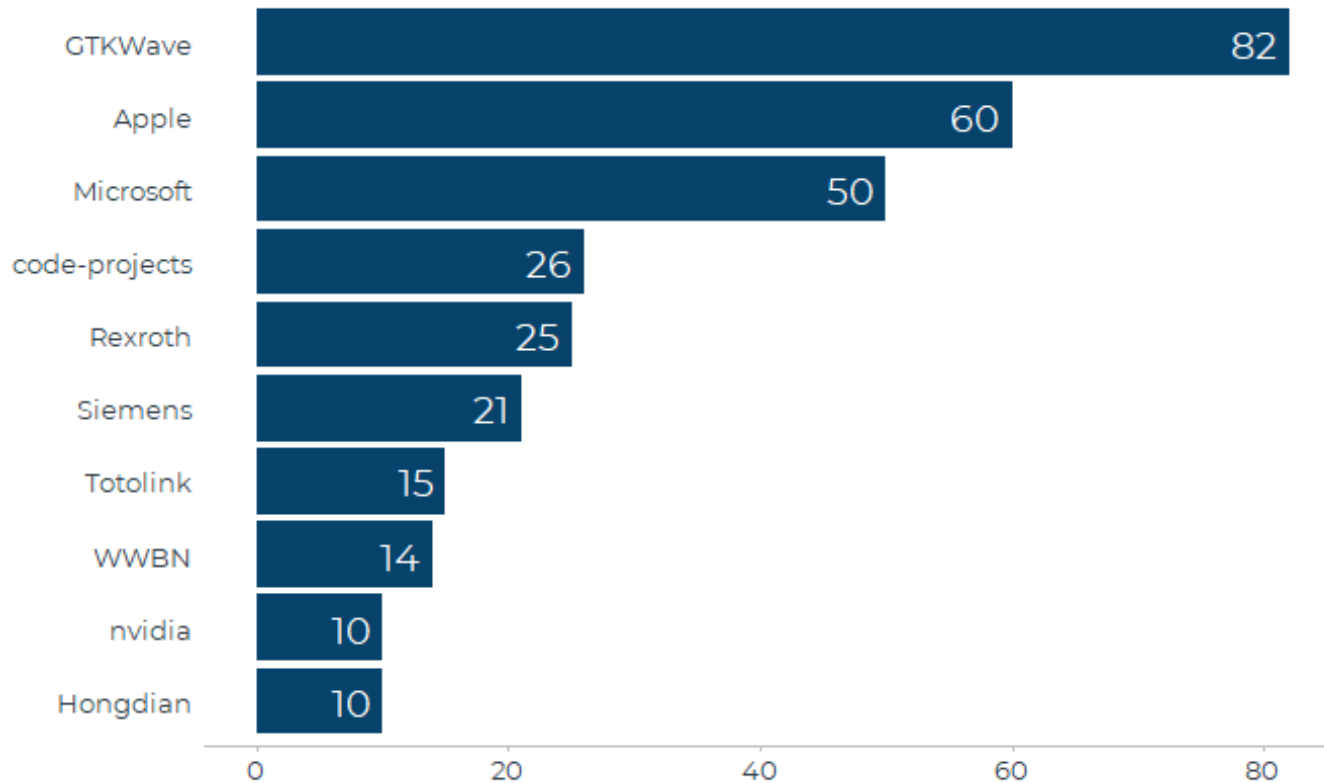
Users can follow the link attached to each CVE number for further information including mitigation or remediation guidance.



Scottish  
Cyber  
Coordination  
Centre

TLP: Clear – Disclosure is not limited.

## Count of vulnerabilities by software vendor (top 10), 8-14 Jan 2024





Scottish  
Cyber  
Coordination  
Centre

TLP: Clear – Disclosure is not limited.

## Vulnerabilities with highest likelihood of exploitation, 8-14 Jan 2024

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
<a href="#">CVE-2022-45354</a>	08-01-2024	WPChill	Download Monitor	5.3	0.006	No
<a href="#">CVE-2023-26999</a>	09-01-2024	n/a	n/a		0.004	No
<a href="#">CVE-2023-50643</a>	09-01-2024	n/a	n/a		0.003	No
<a href="#">CVE-2023-47211</a>	08-01-2024	ManageEngine	OpManager	9.1	0.002	No
<a href="#">CVE-2023-7218</a>	08-01-2024	Totolink	N350RT	7.2	0.002	No
<a href="#">CVE-2023-49236</a>	09-01-2024	n/a	n/a		0.002	No



Scottish  
Cyber  
Coordination  
Centre

TLP: Clear – Disclosure is not limited.

## Vulnerabilities with highest severity, 8-14 Jan 2024

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
<a href="#">CVE-2023-52219</a>	08-01-2024	Gecka	Gecka Terms Thumbnails	9.9	0.001	No
<a href="#">CVE-2024-0252</a>	11-01-2024	ManageEngine	ADSelfService Plus	9.9		No
<a href="#">CVE-2024-21669</a>	11-01-2024	hyperledger	aries-cloudagent-python	9.9		No
<a href="#">CVE-2023-47862</a>	10-01-2024	WWBN	AVideo	9.8		No
<a href="#">CVE-2023-49569</a>	12-01-2024	go-git	go-git	9.8		No
<a href="#">CVE-2023-49599</a>	10-01-2024	WWBN	AVideo	9.8		No
<a href="#">CVE-2023-49621</a>	09-01-2024	Siemens	SIMATIC CN 4100	9.8	0.001	No
<a href="#">CVE-2023-5347</a>	09-01-2024	Korenix	JetNet Series	9.8		No



# Scottish Cyber Coordination Centre

TLP: Clear – Disclosure is not limited.

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
<a href="#">CVE-2023-6316</a>	11-01-2024	inc2734	MW WP Form	9.8		No
<a href="#">CVE-2023-6567</a>	11-01-2024	thimpress	LearnPress – WordPress LMS Plugin	9.8		No
<a href="#">CVE-2023-6875</a>	11-01-2024	wpexpertsio	POST SMTP – The #1 WordPress SMTP Plugin with Advanced Email Logging and Delivery Failure Notifications	9.8		No
<a href="#">CVE-2023-6921</a>	08-01-2024	PrestaShow	PrestaShop Google Integrator	9.8	0.001	No
<a href="#">CVE-2023-6979</a>	11-01-2024	ivole	Customer Reviews for WooCommerce	9.8		No
<a href="#">CVE-2023-7220</a>	09-01-2024	Totolink	NR1800X	9.8	0.001	No
<a href="#">CVE-2023-7221</a>	09-01-2024	Totolink	T6	9.8	0.001	No
<a href="#">CVE-2023-3043</a>	09-01-2024	AMI	MegaRAC_SPx	9.6		No
<a href="#">CVE-2023-</a>	09-01-2024	AMI	MegaRAC_SPx	9.6		No



# Scottish Cyber Coordination Centre

TLP: Clear – Disclosure is not limited.

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
<a href="#">37293</a>						
<a href="#">CVE-2023-39336</a>	09-01-2024	Ivanti	Endpoint Manager	9.6	0.001	No
<a href="#">CVE-2023-48728</a>	10-01-2024	WWBN	AVideo	9.6		No
<a href="#">CVE-2023-51698</a>	12-01-2024	mate-desktop	atril	9.6		No
<a href="#">CVE-2023-52200</a>	08-01-2024	Repute Infosystems	ARMember – Membership Plugin, Content Restriction, Member Levels, User Profile & User signup	9.6	0.001	No
<a href="#">CVE-2023-5356</a>	12-01-2024	GitLab	GitLab	9.6		No
<a href="#">CVE-2023-31029</a>	12-01-2024	nvidia	DGX A100	9.3		No
<a href="#">CVE-2023-31030</a>	12-01-2024	nvidia	DGX A100	9.3		No
<a href="#">CVE-2023-52215</a>	08-01-2024	UkrSolution	Simple Inventory Management – just scan barcode to manage products and orders.	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
			For WooCommerce			
<a href="#">CVE-2024-22199</a>	11-01-2024	gofiber	template	9.3		No
<a href="#">CVE-2023-47211</a>	08-01-2024	ManageEngine	OpManager	9.1	0.002	No
<a href="#">CVE-2023-52202</a>	08-01-2024	SVNLabs Softwares	HTML5 MP3 Player with Folder Feedburner Playlist Free	9.1	0.001	No
<a href="#">CVE-2023-52205</a>	08-01-2024	SVNLabs Softwares	HTML5 SoundCloud Player with Playlist Free	9.1	0.001	No
<a href="#">CVE-2023-52207</a>	08-01-2024	SVNLabs Softwares	HTML5 MP3 Player with Playlist Free	9.1	0.001	No
<a href="#">CVE-2023-6699</a>	11-01-2024	smartersite	WP Compress – Image Optimizer [All-In-One]	9.1		No
<a href="#">CVE-2024-0057</a>	09-01-2024	Microsoft	.NET 8.0	9.1		No
<a href="#">CVE-2024-21638</a>	10-01-2024	Azure	ipam	9.1		No



# Scottish Cyber Coordination Centre

TLP: Clear – Disclosure is not limited.

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
<a href="#">CVE-2024-21887</a>	12-01-2024	Ivanti	ICS	9.1		Yes
<a href="#">CVE-2024-22206</a>	12-01-2024	clerk	javascript	9.1		No
<a href="#">CVE-2023-31024</a>	12-01-2024	nvidia	DGX A100	9		No
<a href="#">CVE-2023-47861</a>	10-01-2024	WWBN	AVideo	9		No
<a href="#">CVE-2023-50982</a>	08-01-2024	n/a	n/a	9	0.001	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](mailto:SC3@gov.scot)