



Scottish  
Cyber  
Coordination  
Centre

TLP: Clear

# Weekly Vulnerability Report

30 January 2024

This report summarizes the known software vulnerabilities published during the period **22 to 28 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 and a table of vulnerabilities with the highest severity rating ([CVSSv3](#) Base Score  $\geq 9$ ). The table 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.

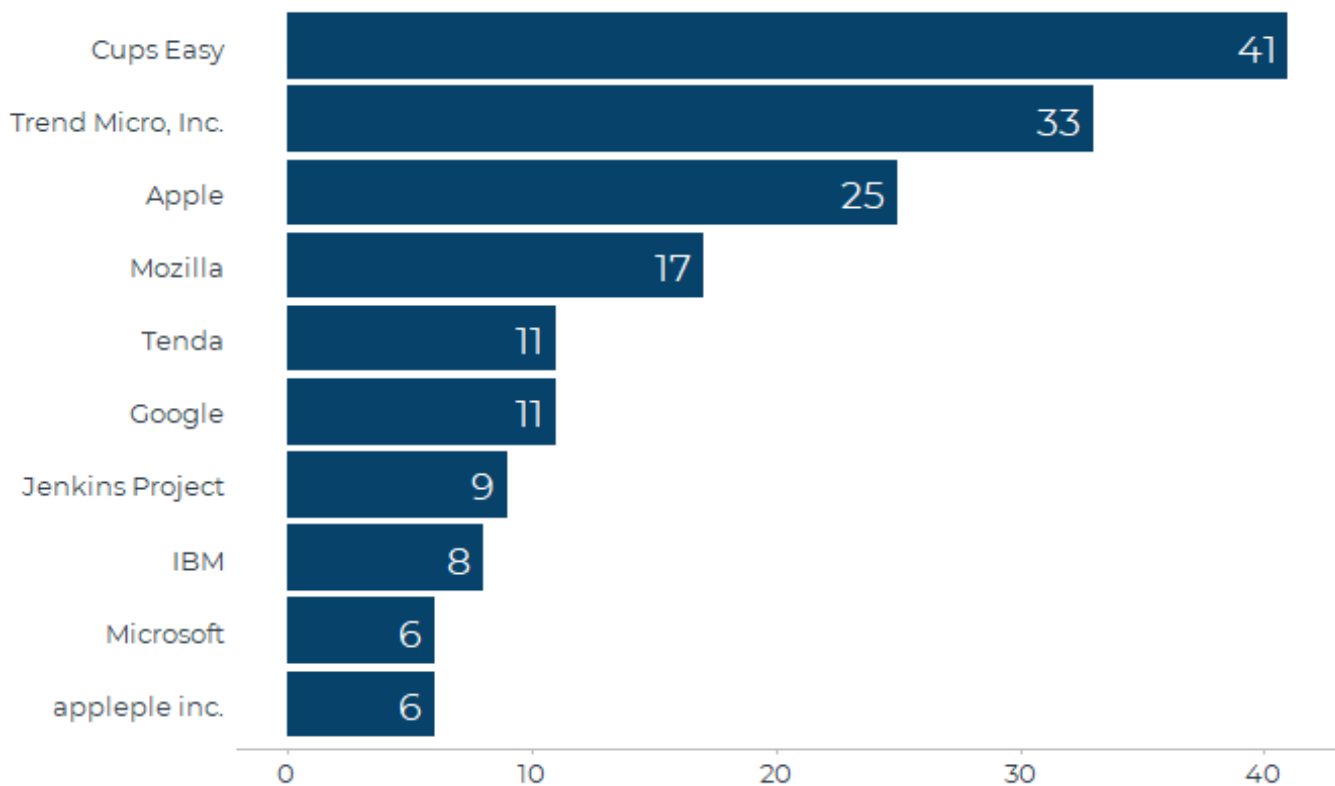
**We would like to know what you think about the weekly vulnerability report. Please take a few minutes to complete this anonymous [survey](#).**



Scottish  
Cyber  
Coordination  
Centre

TLP: Clear

## Count of vulnerabilities by software vendor (top 10), 22-28 Jan 2024





Scottish  
Cyber  
Coordination  
Centre

TLP: Clear

## Vulnerabilities with highest severity, 22-28 Jan 2024

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
<a href="#">CVE-2024-0402</a>	26-01-2024	GitLab	GitLab	9.9		No
<a href="#">CVE-2024-20253</a>	26-01-2024	Cisco	Cisco Unified Contact Center Enterprise	9.9		No
<a href="#">CVE-2023-7227</a>	25-01-2024	SystemK	NVR 504	9.8		No
<a href="#">CVE-2024-0204</a>	22-01-2024	Fortra	GoAnywhere MFT	9.8	0.001	No
<a href="#">CVE-2024-23619</a>	25-01-2024	IBM Merge Healthcare	eFilm Workstation	9.8		No
<a href="#">CVE-2024-23636</a>	23-01-2024	sofastack	sofa-rpc	9.8		No
<a href="#">CVE-2023-49657</a>	23-01-2024	Apache Software Foundation	Apache Superset	9.6		No
<a href="#">CVE-2024-21326</a>	26-01-2024	Microsoft	Microsoft Edge (Chromium-based)	9.6		No
<a href="#">CVE-2024-</a>	25-01-2024	Symantec	Data Loss Prevention	9.6		No



# Scottish Cyber Coordination Centre

TLP: Clear

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
<a href="#">23617</a>						
<a href="#">CVE-2024-23618</a>	25-01-2024	Arris	SURFboard SBG6950AC2	9.6		No
<a href="#">CVE-2024-23624</a>	25-01-2024	D-Link	DAP-1650	9.6		No
<a href="#">CVE-2024-23625</a>	25-01-2024	D-Link	DAP-1650	9.6		No
<a href="#">CVE-2024-23629</a>	25-01-2024	Motorola	MR2600	9.6		No
<a href="#">CVE-2024-22203</a>	23-01-2024	benbusby	whoogle-search	9.1		No
<a href="#">CVE-2024-22205</a>	23-01-2024	benbusby	whoogle-search	9.1		No
<a href="#">CVE-2024-23626</a>	25-01-2024	Motorola	MR2600	9		No
<a href="#">CVE-2024-23627</a>	25-01-2024	Motorola	MR2600	9		No
<a href="#">CVE-2024-23628</a>	25-01-2024	Motorola	MR2600	9		No



# Scottish Cyber Coordination Centre

TLP: Clear

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
<a href="#">CVE-2024-23630</a>	25-01-2024	Motorola	MR2600	9		No



Scottish  
Cyber  
Coordination  
Centre

TLP: Clear

## 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)