Scottish
Cyber
Coordination
Centre

TLP: CLEAR

Weekly Vulnerability Report

6 February 2024

This report summarizes the known software vulnerabilities published during the period **29 January to 4 Feb 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).

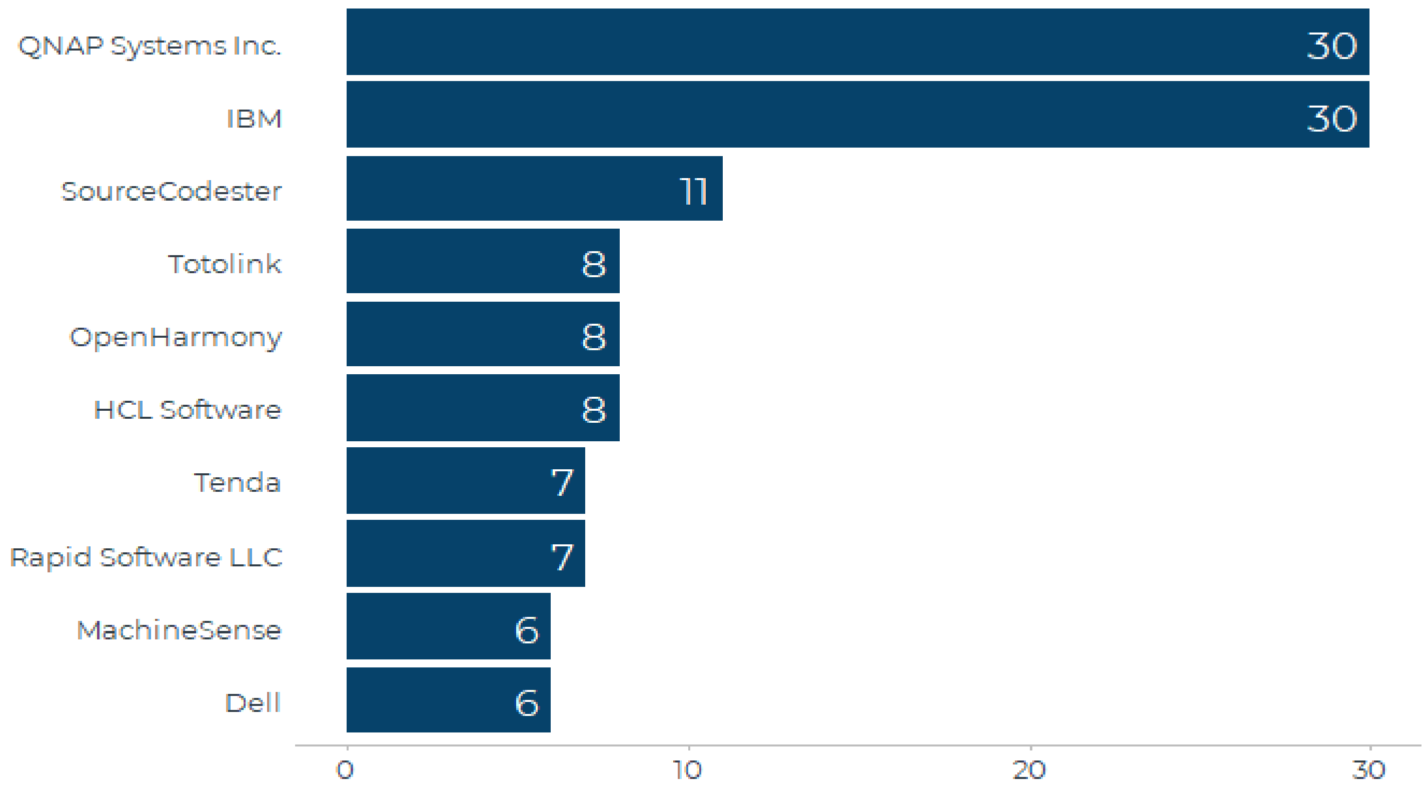
Users can follow the link attached to each CVE number for further information including mitigation or remediation guidance.

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), 29 Jan-4 Feb 2024



Vulnerabilities with highest likelihood of exploitation, 29 Jan-4 Feb 2024

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-24324	30-01-2024	Totolink	n/a		0.066	No
CVE-2024-24325	30-01-2024	Totolink	n/a		0.004	No
CVE-2024-24326	30-01-2024	Totolink	n/a		0.004	No
CVE-2024-24327	30-01-2024	Totolink	n/a		0.004	No
CVE-2024-24328	30-01-2024	Totolink	n/a		0.004	No
CVE-2024-24329	30-01-2024	Totolink	n/a		0.004	No
CVE-2024-24330	30-01-2024	Totolink	n/a		0.004	No
CVE-2024-24331	30-01-2024	Totolink	n/a		0.004	No

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-24332	30-01-2024	Totolink	n/a		0.004	No
CVE-2024-24333	30-01-2024	Totolink	n/a		0.004	No
CVE-2024-1015	29-01-2024	SE-elektronic GmbH	E-DDC3.3	9.8	0.003	No
CVE-2024-0989	29-01-2024	Sichuan Yougou Technology	KuERP	5.4	0.002	No
CVE-2024-0997	29-01-2024	Totolink	N200RE	7.2	0.002	No
CVE-2024-0998	29-01-2024	Totolink	N200RE	7.2	0.002	No
CVE-2024-0999	29-01-2024	Totolink	N200RE	7.2	0.002	No
CVE-2024-1002	29-01-2024	Totolink	N200RE	7.2	0.002	No
CVE-2024-1003	29-01-2024	Totolink	N200RE	7.2	0.002	No

TLP: CLEAR

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-1004	29-01-2024	Totolink	N200RE	7.2	0.002	No

Vulnerabilities with highest severity, 29 Jan-4 Feb 2024

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2023-6675	02-02-2024	National Keep Cyber Security Services	CyberMath	9.8		No
CVE-2023-6943	30-01-2024	Mitsubishi Electric Corporation	EZSocket	9.8		No
CVE-2024-1015	29-01-2024	SE-elektronic GmbH	E-DDC3.3	9.8	0.003	No
CVE-2024-1039	01-02-2024	Gessler GmbH	WEB-MASTER	9.8		No
CVE-2024-21764	01-02-2024	Rapid Software LLC	Rapid SCADA	9.8		No
CVE-2024-21917	31-01-2024	Rockwell Automation	FactoryTalk® Service Platform	9.8		No
CVE-2024-22320	02-02-2024	IBM	Operational Decision Manager	9.8		No
CVE-2024-23653	31-01-2024	moby	buildkit	9.8		No

CVE	Date Published	Vendor	Product	Base Score	Probability of Exploitation	Exploited
CVE-2024-23827	29-01-2024	0xJacky	nginx-ui	9.8		No
CVE-2024-24561	01-02-2024	vyperlang	vyper	9.8		No
CVE-2024-23832	01-02-2024	mastodon	mastodon	9.4		No
CVE-2022-34381	02-02-2024	Dell	Dell BSAFE Crypto-J	9.1		No
CVE-2023-46706	01-02-2024	MachineSense	FeverWarn	9.1		No
CVE-2023-50356	31-01-2024	AREAL SAS	Topkapi Vision (Server)	9.1		No
CVE-2023-5389	30-01-2024	Honeywell	ControlEdge UOC	9.1		No
CVE-2024-23328	01-02-2024	dataease	dataease	9.1		No
CVE-2023-45025	02-02-2024	QNAP Systems Inc.	QTS	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