



Scottish
Cyber
Coordination
Centre

Weekly Vulnerability Report

16 July 2024

This report summarizes the known software vulnerabilities published during the period **8-14 July 2024**. This data can help users prioritise and manage the vulnerabilities that might pose a risk to their organisations.

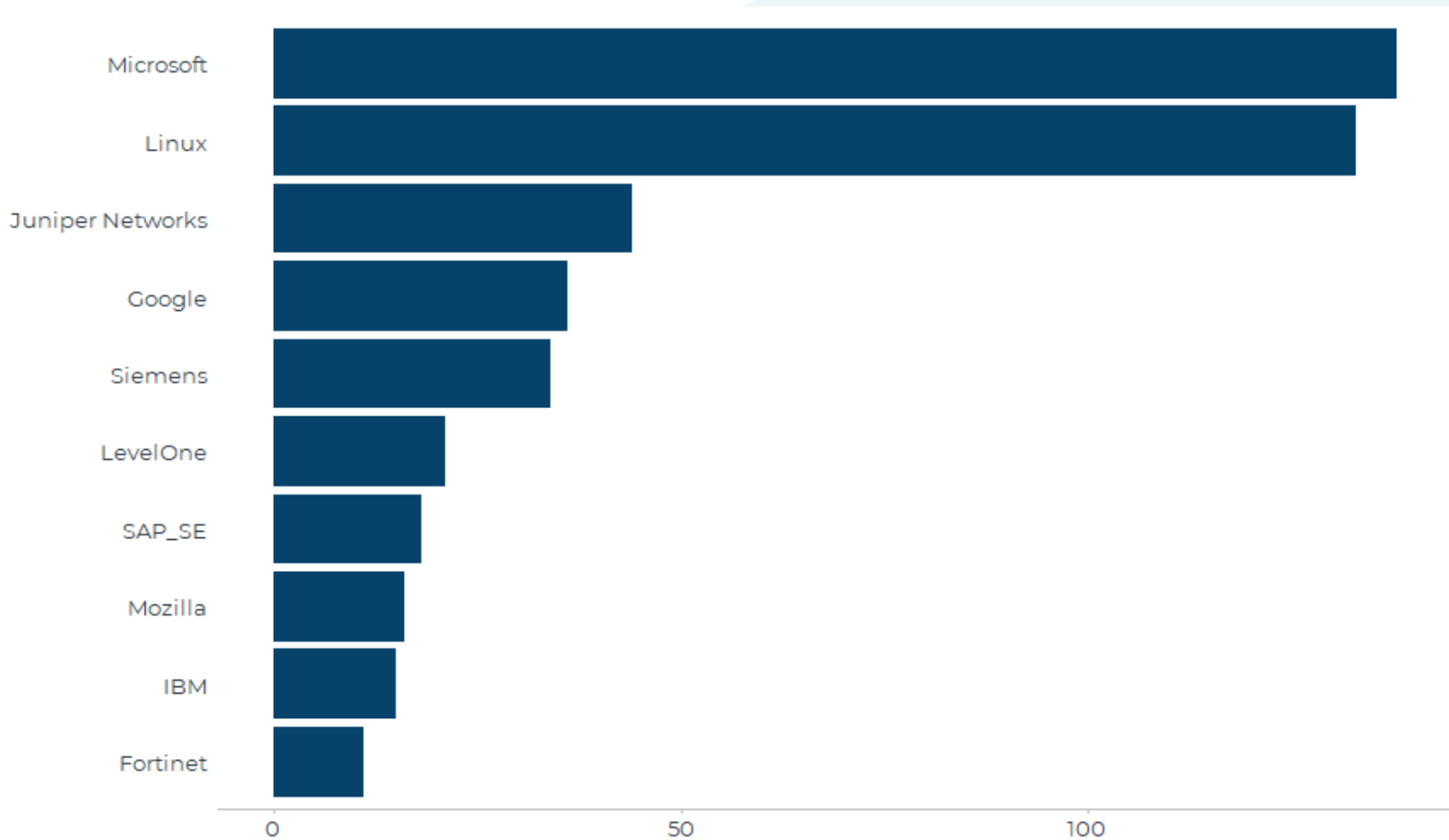
It includes a breakdown of vulnerabilities by vendor, a table of vulnerabilities with the highest likelihood of being exploited ([EPSS >0.001](#)), and a table of vulnerabilities with the highest severity rating ([CVSSv3 Base Score >=9](#)). The tables also indicate whether a vulnerability has been exploited 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.

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



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





Vulnerabilities with highest likelihood of exploitation, 8-14 July 2024

| CVE | Date Published | Vendor | Product | Base Score | Probability of Exploitation | Exploited |
|----------------|----------------|-----------|-------------------------|------------|-----------------------------|-----------|
| CVE-2024-38112 | 09-07-2024 | Microsoft | Windows 10 Version 22H2 | 7.5 | 0.016 | Yes |
| CVE-2024-38020 | 09-07-2024 | Microsoft | Microsoft Office 2019 | 6.5 | 0.003 | No |
| CVE-2024-38030 | 09-07-2024 | Microsoft | Windows 10 Version 1809 | 6.5 | 0.003 | No |
| CVE-2024-38049 | 09-07-2024 | Microsoft | Windows 10 Version 1809 | 6.6 | 0.003 | No |
| CVE-2024-38072 | 09-07-2024 | Microsoft | Windows Server 2019 | 7.5 | 0.002 | No |
| CVE-2024-39171 | 09-07-2024 | n/a | n/a | 8.8 | 0.002 | No |
| CVE-2024-38074 | 09-07-2024 | Microsoft | Windows Server 2019 | 9.8 | 0.001 | No |
| CVE-2024-38076 | 09-07-2024 | Microsoft | Windows Server 2019 | 9.8 | 0.001 | No |
| CVE-2024-38077 | 09-07-2024 | Microsoft | Windows Server 2019 | 9.8 | 0.001 | No |
| CVE-2024-38064 | 09-07-2024 | Microsoft | Windows 10 Version 1809 | 7.5 | 0.001 | No |
| CVE-2024-6385 | 11-07-2024 | GitLab | GitLab | 9.6 | 0.001 | No |



| CVE | Date Published | Vendor | Product | Base Score | Probability of Exploitation | Exploited |
|----------------|----------------|-----------|-------------------------|------------|-----------------------------|-----------|
| CVE-2023-48194 | 09-07-2024 | n/a | n/a | 6.3 | 0.001 | No |
| CVE-2024-38021 | 09-07-2024 | Microsoft | Microsoft Office 2019 | 8.8 | 0.001 | No |
| CVE-2024-38104 | 09-07-2024 | Microsoft | Windows 10 Version 1809 | 8.8 | 0.001 | No |
| CVE-2024-40539 | 12-07-2024 | n/a | n/a | 6.2 | 0.001 | No |
| CVE-2024-40540 | 12-07-2024 | n/a | n/a | 6.2 | 0.001 | No |
| CVE-2024-40541 | 12-07-2024 | n/a | n/a | 6.2 | 0.001 | No |
| CVE-2024-40542 | 12-07-2024 | n/a | n/a | 6.3 | 0.001 | No |



Vulnerabilities with highest severity, 8-14 July 2024

| CVE | Date Published | Vendor | Product | Base Score | Probability of Exploitation | Exploited |
|----------------|----------------|------------------|-----------------------------|------------|-----------------------------|-----------|
| CVE-2023-3287 | 09-07-2024 | easyappointments | easyappointments | 9.9 | | No |
| CVE-2023-38048 | 09-07-2024 | easyappointments | easyappointments | 9.9 | | No |
| CVE-2023-38049 | 09-07-2024 | NA | easyappointments | 9.9 | | No |
| CVE-2023-38051 | 09-07-2024 | easyappointments | easyappointments | 9.9 | | No |
| CVE-2023-38052 | 09-07-2024 | easyappointments | easyappointments | 9.9 | | No |
| CVE-2023-38053 | 09-07-2024 | easyappointments | easyappointments | 9.9 | | No |
| CVE-2023-38054 | 09-07-2024 | alextselegidis | easyappointments | 9.9 | | No |
| CVE-2024-3604 | 09-07-2024 | photoweblog | OSM – OpenStreetMap | 9.9 | | No |
| CVE-2024-37418 | 09-07-2024 | Andy Moyle | Church Admin | 9.9 | | No |
| CVE-2024-37420 | 09-07-2024 | WPZita | Zita Elementor Site Library | 9.9 | | No |



| CVE | Date Published | Vendor | Product | Base Score | Probability of Exploitation | Exploited |
|----------------|----------------|----------------------------|---------------------------|------------|-----------------------------|-----------|
| CVE-2024-37424 | 09-07-2024 | Automattic | Newspack Blocks | 9.9 | | No |
| CVE-2023-46685 | 08-07-2024 | LevelOne | WBR-6013 | 9.8 | 0.001 | No |
| CVE-2024-1305 | 08-07-2024 | OpenVPN | tap-windows6 | 9.8 | | No |
| CVE-2024-28747 | 09-07-2024 | ifm | Smart PLC AC14xx Firmware | 9.8 | 0.001 | No |
| CVE-2024-36435 | 11-07-2024 | n/a | n/a | 9.8 | | No |
| CVE-2024-36522 | 12-07-2024 | Apache Software Foundation | Apache Wicket | 9.8 | | No |
| CVE-2024-37113 | 10-07-2024 | Membership Software | WishList Member X | 9.8 | | No |
| CVE-2024-37870 | 09-07-2024 | n/a | n/a | 9.8 | | No |
| CVE-2024-37927 | 12-07-2024 | NooTheme | Jobmonster | 9.8 | | No |
| CVE-2024-38074 | 09-07-2024 | Microsoft | Windows Server 2019 | 9.8 | 0.001 | No |
| CVE-2024-38076 | 09-07-2024 | Microsoft | Windows Server 2019 | 9.8 | 0.001 | No |



| CVE | Date Published | Vendor | Product | Base Score | Probability of Exploitation | Exploited |
|----------------|----------------|--------------------|------------------------------------------------------------|------------|-----------------------------|-----------|
| CVE-2024-38077 | 09-07-2024 | Microsoft | Windows Server 2019 | 9.8 | 0.001 | No |
| CVE-2024-39071 | 09-07-2024 | n/a | n/a | 9.8 | | No |
| CVE-2024-39914 | 12-07-2024 | FOGProject | fogproject | 9.8 | | No |
| CVE-2024-5488 | 09-07-2024 | Unknown | SEOPress | 9.8 | | No |
| CVE-2024-6313 | 09-07-2024 | nikolaystrikhar | Gutenberg Forms – WordPress Form Builder Plugin | 9.8 | 0.001 | No |
| CVE-2024-6314 | 09-07-2024 | rmac0001 | IQ Testimonials | 9.8 | 0.001 | No |
| CVE-2024-6328 | 12-07-2024 | inspireui | MStore API – Create Native Android & iOS Apps On The Cloud | 9.8 | 0.001 | No |
| CVE-2024-6365 | 09-07-2024 | woobewoo | Product Table by WBW | 9.8 | 0.001 | No |
| CVE-2024-6396 | 12-07-2024 | aimhubio | aimhubio/aim | 9.8 | | No |
| CVE-2024-6397 | 11-07-2024 | instawp | InstaWP Connect – 1-click WP Staging & Migration | 9.8 | 0.001 | No |
| CVE-2024-6407 | 11-07-2024 | Schneider Electric | Wiser Home Controller WHC-5918A | 9.8 | 0.001 | No |



| CVE | Date Published | Vendor | Product | Base Score | Probability of Exploitation | Exploited |
|----------------|----------------|------------------|------------------------------|------------|-----------------------------|-----------|
| CVE-2024-6422 | 10-07-2024 | Pepperl+Fuchs | OIT1500-F113-B12-CB | 9.8 | 0.001 | No |
| CVE-2024-6602 | 09-07-2024 | Mozilla | Firefox | 9.8 | | No |
| CVE-2024-6606 | 09-07-2024 | Mozilla | Firefox | 9.8 | | No |
| CVE-2024-6611 | 09-07-2024 | Mozilla | Firefox | 9.8 | | No |
| CVE-2024-6624 | 11-07-2024 | parorrey | JSON API User | 9.8 | 0.001 | No |
| CVE-2023-38055 | 09-07-2024 | easyappointments | easyappointments | 9.6 | | No |
| CVE-2024-39872 | 09-07-2024 | Siemens | SINEMA Remote Connect Server | 9.6 | | No |
| CVE-2024-40618 | 11-07-2024 | NAVER | NAVER Whale browser | 9.6 | | No |
| CVE-2024-6385 | 11-07-2024 | GitLab | GitLab | 9.6 | 0.001 | No |
| CVE-2024-6235 | 10-07-2024 | NetScaler | NetScaler Console | 9.4 | | No |
| CVE-2024-37933 | 12-07-2024 | anhvnit | Woocommerce OpenPos | 9.3 | | No |



| CVE | Date Published | Vendor | Product | Base Score | Probability of Exploitation | Exploited |
|----------------|----------------|--------------------|-----------------------------------|------------|-----------------------------|-----------|
| CVE-2024-4879 | 10-07-2024 | ServiceNow | Now Platform | 9.3 | 0.001 | No |
| CVE-2024-5910 | 10-07-2024 | Palo Alto Networks | Expedition | 9.3 | | No |
| CVE-2024-6035 | 11-07-2024 | gaizhenbiao | gaizhenbiao/chuanhuchatgpt | 9.3 | | No |
| CVE-2024-6527 | 09-07-2024 | Jan Syski | MegaBIP | 9.3 | | No |
| CVE-2024-5217 | 10-07-2024 | ServiceNow | Now Platform | 9.2 | 0.001 | No |
| CVE-2023-38050 | 09-07-2024 | NA | easyappointments | 9.1 | | No |
| CVE-2024-28751 | 09-07-2024 | ifm | Smart PLC AC14xx Firmware | 9.1 | 0.001 | No |
| CVE-2024-37310 | 10-07-2024 | Everest | everest-core | 9.1 | | No |
| CVE-2024-37555 | 09-07-2024 | ZealousWeb | Generate PDF using Contact Form 7 | 9.1 | | No |
| CVE-2024-37770 | 10-07-2024 | n/a | n/a | 9.1 | | No |
| CVE-2024-38089 | 09-07-2024 | Microsoft | Microsoft Defender for IoT | 9.1 | | No |



Scottish
Cyber
Coordination
Centre

| CVE | Date Published | Vendor | Product | Base Score | Probability of Exploitation | Exploited |
|----------------|----------------|----------------------|------------------------------------------|------------|-----------------------------|-----------|
| CVE-2024-38734 | 12-07-2024 | SpreadsheetConverter | Import Spreadsheets from Microsoft Excel | 9.1 | | No |
| CVE-2024-38736 | 12-07-2024 | Realtyna | Realtyna Organic IDX plugin | 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