# Microsoft Defender Vulnerability Management

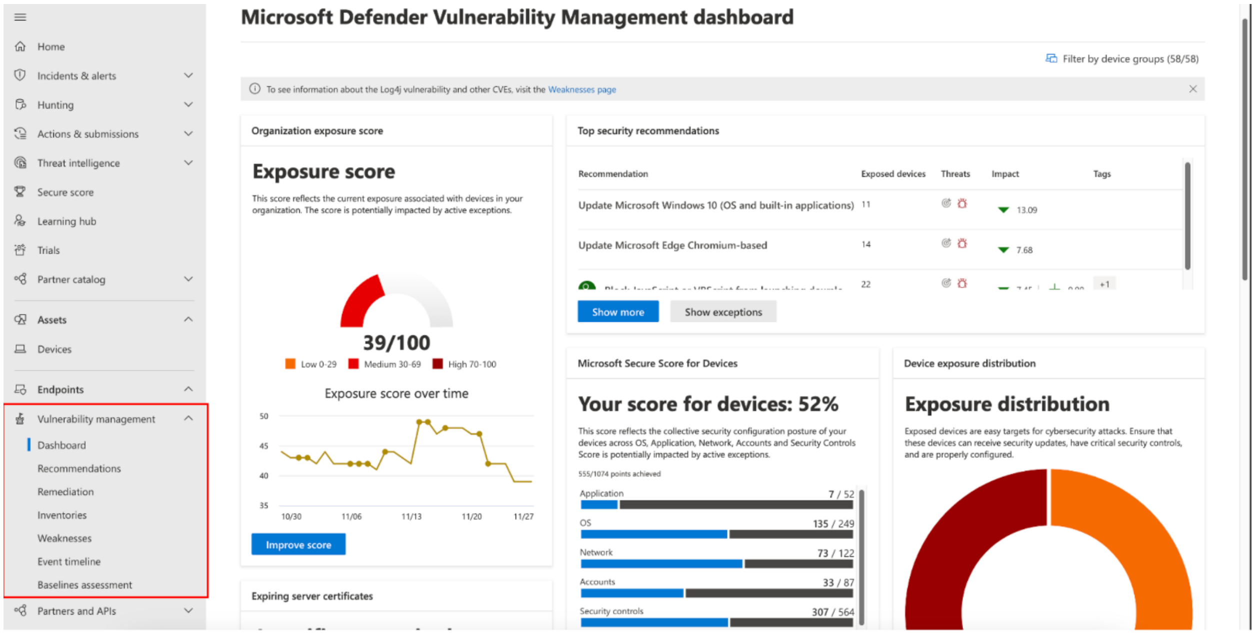
Vulnerability management is a proactive cybersecurity practice aimed at identifying, evaluating, treating, and reporting security vulnerabilities in systems and software. It involves a systematic approach to discovering potential weaknesses through various methods such as scanning and testing, followed by assessing the risks associated with each vulnerability. The process prioritizes vulnerabilities based on their severity and potential impact, allowing organizations to allocate resources effectively for remediation. This includes applying patches, reconfiguring systems, or implementing additional security measures. Continuous monitoring and periodic reviews are crucial to ensure that new vulnerabilities are promptly addressed, thereby maintaining a robust security posture and protecting sensitive data from potential threats.

Microsoft Defender Vulnerability Management is an advanced security solution integrated into Microsoft Defender for Endpoint, designed to enhance an organization's vulnerability management efforts. It provides comprehensive capabilities for identifying, assessing, and mitigating vulnerabilities across various endpoints and devices. Key features include continuous vulnerability scanning, real-time risk assessment, and actionable insights that prioritize vulnerabilities based on their potential impact.

The platform offers detailed remediation guidance, integrated patch management, and automated workflows to streamline the resolution process. Additionally, it provides in-depth visibility into the security posture of an organization's IT environment, allowing for proactive defense against emerging threats. With its seamless integration into the broader Microsoft 365 security ecosystem, Microsoft Defender Vulnerability Management helps organizations maintain a strong security posture and reduce the attack surface.

# Examples: -

1. **Dashboard**: Provides information about vulnerabilities, exposure, and recommendations. You can see recent remediation activities, exposed devices, and ways to improve your company's overall security. Each card in the dashboard includes a link to more detailed information or to a page where you can take a recommended action.



### Microsoft Defender Vulnerability Management dashboard

To see information about the Log4j vulnerability and other CVEs, visit the Weaknesses page

**Exposure score**

This score reflects the current exposure associated with devices in your organization. The score is potentially impacted by active exceptions.

| Recommendation | Exposed devices | Threats | Impact | Tags |
|---|---|---|---|---|
| Update Microsoft Windows 10 (OS and built-in applications) | 11 | | 13.09 | |
| Update Microsoft Edge Chromium-based | 14 | | 7.68 | |
| Block JavaScript or VBScript from launching downloade | 22 | | 7.45 0.00 | +1 |

**Your score for devices: 52%**

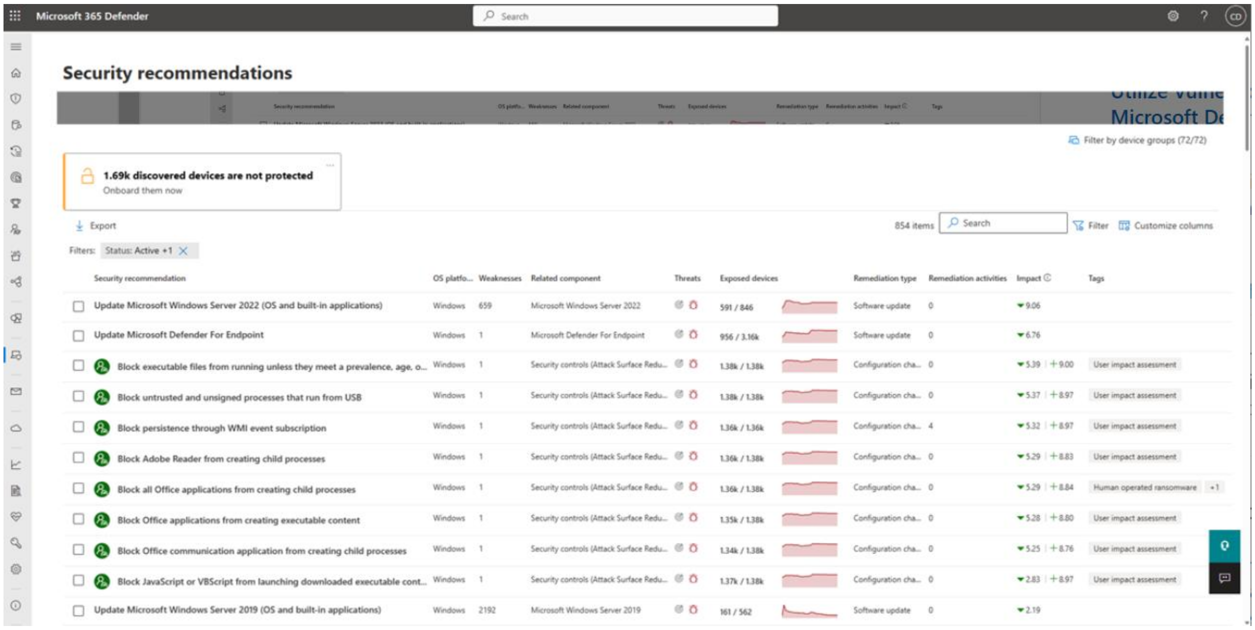
This score reflects the collective security configuration posture of your devices across OS, Application, Network, Accounts and Security Controls Score is potentially impacted by active exceptions.

555/1074 points achieved

**Exposure distribution**

Exposed devices are easy targets for cybersecurity attacks. Ensure that these devices can receive security updates, have critical security controls, and are properly configured.

2. **Recommendations**: Lists current security recommendations and related threat information to review and consider. When you select an item in the list, a flyout panel opens with more details about threats and actions you can take.



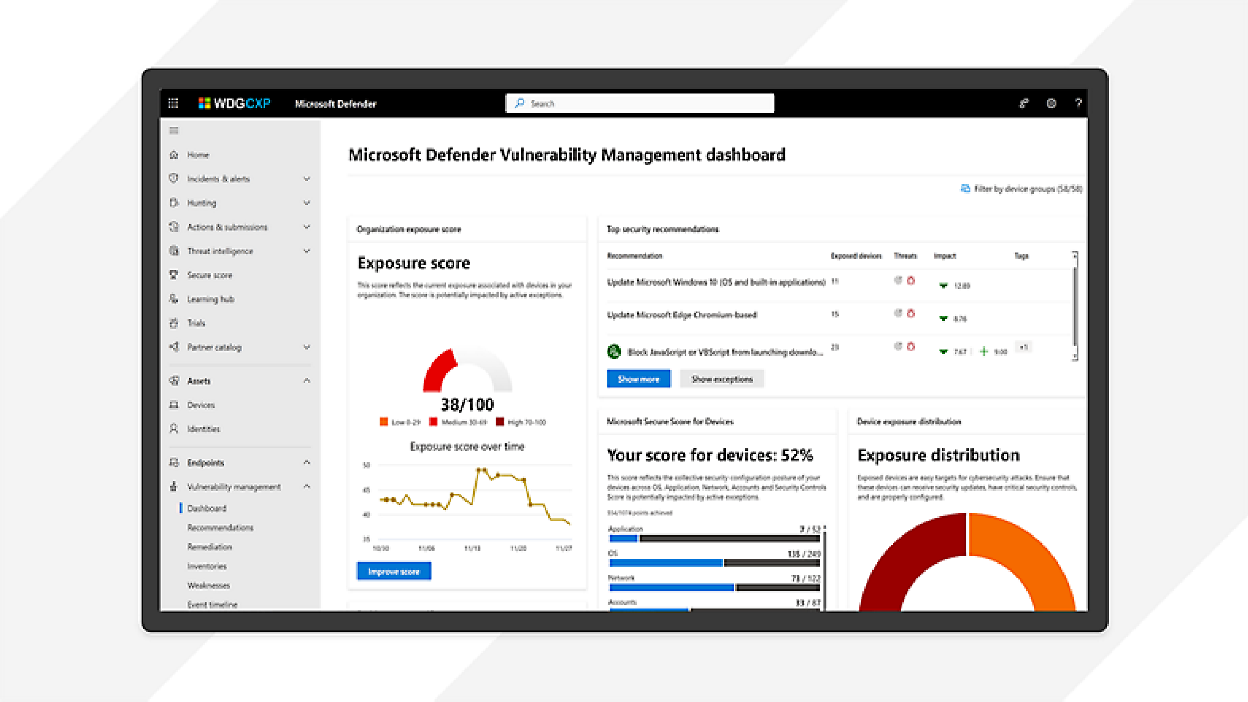
Security recommendations

1.69k discovered devices are not protected
Onboard them now

Filters: Status: Active +1

| | Security recommendation | OS platfo... | Weaknesses | Related component | Threats | Exposed devices | Remediation type | Remediation activities | Impact | Tags |
|---|---|---|---|---|---|---|---|---|---|---|
| □ | Update Microsoft Windows Server 2022 (OS and built-in applications) | Windows | 659 | Microsoft Windows Server 2022 | | 591 / 846 | Software update | 0 | ▼9.06 | |
| □ | Update Microsoft Defender For Endpoint | Windows | 1 | Microsoft Defender For Endpoint | | 956 / 3.16k | Software update | 0 | ▼6.76 | |
| □ | Block executable files from running unless they meet a prevalence, age, o... | Windows | 1 | Security controls (Attack Surface Redu... | | 1.38k / 1.38k | Configuration cha... | 0 | ▼5.39 \| +9.00 | User impact assessment |
| □ | Block untrusted and unsigned processes that run from USB | Windows | 1 | Security controls (Attack Surface Redu... | | 1.38k / 1.38k | Configuration cha... | 0 | ▼5.37 \| +8.97 | User impact assessment |
| □ | Block persistence through WMI event subscription | Windows | 1 | Security controls (Attack Surface Redu... | | 1.36k / 1.36k | Configuration cha... | 4 | ▼5.32 \| +8.97 | User impact assessment |
| □ | Block Adobe Reader from creating child processes | Windows | 1 | Security controls (Attack Surface Redu... | | 1.36k / 1.38k | Configuration cha... | 0 | ▼5.29 \| +8.83 | User impact assessment |
| □ | Block all Office applications from creating child processes | Windows | 1 | Security controls (Attack Surface Redu... | | 1.36k / 1.38k | Configuration cha... | 0 | ▼5.29 \| +8.84 | Human operated ransomware +1 |
| □ | Block Office applications from creating executable content | Windows | 1 | Security controls (Attack Surface Redu... | | 1.35k / 1.38k | Configuration cha... | 0 | ▼5.28 \| +8.80 | User impact assessment |
| □ | Block Office communication application from creating child processes | Windows | 1 | Security controls (Attack Surface Redu... | | 1.34k / 1.38k | Configuration cha... | 0 | ▼5.25 \| +8.76 | User impact assessment |
| □ | Block JavaScript or VBScript from launching downloaded executable cont... | Windows | 1 | Security controls (Attack Surface Redu... | | 1.37k / 1.38k | Configuration cha... | 0 | ▼2.83 \| +8.97 | User impact assessment |
| □ | Update Microsoft Windows Server 2019 (OS and built-in applications) | Windows | 2192 | Microsoft Windows Server 2019 | | 161 / 562 | Software update | 0 | ▼2.19 | |

3. **Remediation**: Lists any remediation actions and their status. Remediation activities can include sending a file to quarantine, stopping a process from running, and blocking a detected threat from running. Remediation activities can also include updating a device, running an antivirus scan, and more.



Microsoft Defender Vulnerability Management dashboard

Exposure score

This score reflects the current exposure associated with devices in your organization. The score is potentially impacted by active exceptions.

| Recommendation | Exposed devices | Threats | Impact | Tags |
|---|---|---|---|---|
| Update Microsoft Windows 10 (OS and built-in applications) | 11 | | 12.89 | |
| Update Microsoft Edge Chromium-based | 15 | | 8.76 | |
| Block JavaScript or VBScript from launching downlo... | 23 | | 7.67 + 9.00 | +1 |

Your score for devices: 52%

This score reflects the collective security configuration posture of your devices across OS, Application, Network, Accounts and Security Controls. Score is potentially impacted by active exceptions.

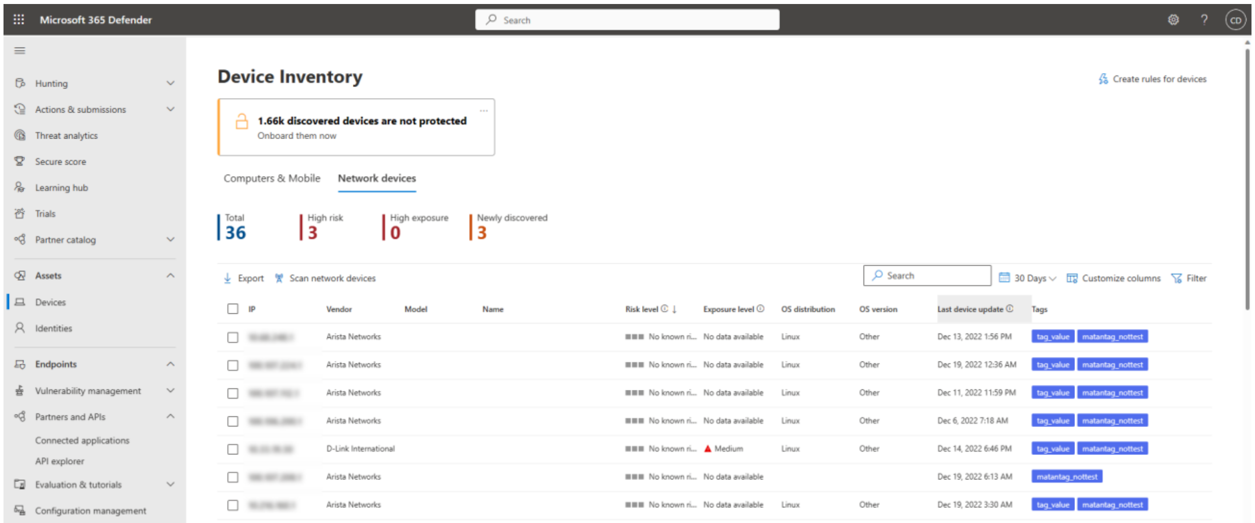
554/1074 points achieved

| | |
|---|---|
| Application | 7 / 52 |
| OS | 135 / 249 |
| Network | 71 / 122 |
| Accounts | 33 / 87 |

Exposure distribution

Exposed devices are easy targets for cybersecurity attacks. Ensure that these devices can receive security updates, have critical security controls, and are properly configured.

4. **Inventories**: Lists software and apps currently in use in your organization. You'll see browsers, operating systems, and other software on devices, along with identified weaknesses and threats.



Device Inventory

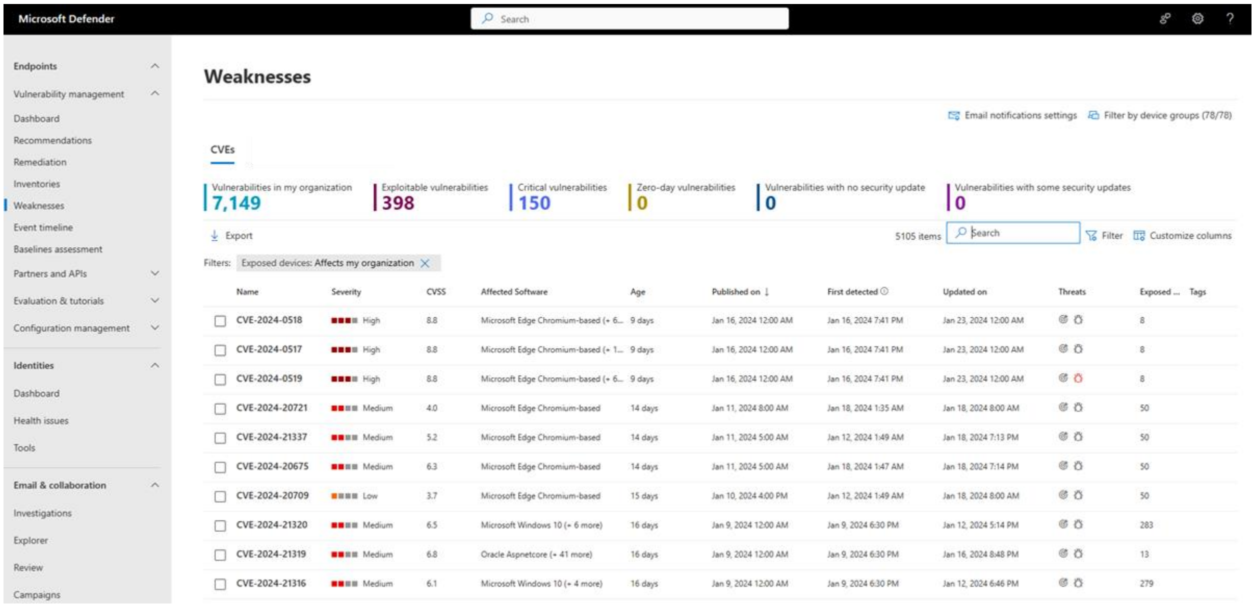
1.66k discovered devices are not protected
Onboard them now

Computers & Mobile | Network devices

Total 36 | High risk 3 | High exposure 0 | Newly discovered 3

| □ | IP | Vendor | Model | Name | Risk level | Exposure level | OS distribution | OS version | Last device update | Tags |
|---|---|---|---|---|---|---|---|---|---|---|
| □ | [redacted] | Arista Networks | | | No known ri... | No data available | Linux | Other | Dec 13, 2022 1:56 PM | tag_value matantag_nottest |
| □ | [redacted] | Arista Networks | | | No known ri... | No data available | Linux | Other | Dec 19, 2022 12:36 AM | tag_value matantag_nottest |
| □ | [redacted] | Arista Networks | | | No known ri... | No data available | Linux | Other | Dec 11, 2022 11:59 PM | tag_value matantag_nottest |
| □ | [redacted] | Arista Networks | | | No known ri... | No data available | Linux | Other | Dec 6, 2022 7:18 AM | tag_value matantag_nottest |
| □ | [redacted] | D-Link International | | | No known ri... | ▲ Medium | Linux | Other | Dec 14, 2022 6:46 PM | tag_value matantag_nottest |
| □ | [redacted] | Arista Networks | | | No known ri... | No data available | | | Dec 19, 2022 6:13 AM | matantag_nottest |
| □ | [redacted] | Arista Networks | | | No known ri... | No data available | Linux | Other | Dec 19, 2022 3:30 AM | tag_value matantag_nottest |

5. **Weaknesses**: Lists vulnerabilities along with the number of exposed devices in your organization. If you see "0" in the Exposed devices column, you do not have to take any immediate action. However, you can learn more about each vulnerability listed on this page. Select an item to learn more about it and what you can do to mitigate the potential threat to your company.



Weaknesses

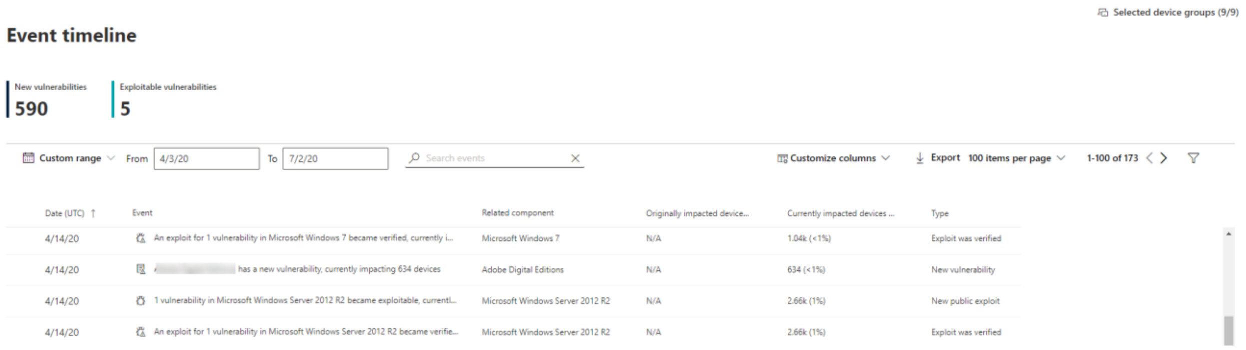
Vulnerabilities in my organization 7,149 | Exploitable vulnerabilities 398 | Critical vulnerabilities 150 | Zero-day vulnerabilities 0 | Vulnerabilities with no security update 0 | Vulnerabilities with some security updates 0

5105 items

Filters: Exposed devices: Affects my organization

| | Name | Severity | CVSS | Affected Software | Age | Published on ↓ | First detected | Updated on | Threats | Exposed ... | Tags |
|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | CVE-2024-0518 | High | 8.8 | Microsoft Edge Chromium-based (+ 6... | 9 days | Jan 16, 2024 12:00 AM | Jan 16, 2024 7:41 PM | Jan 23, 2024 12:00 AM | | 8 | |
| □ | CVE-2024-0517 | High | 8.8 | Microsoft Edge Chromium-based (+ 1... | 9 days | Jan 16, 2024 12:00 AM | Jan 16, 2024 7:41 PM | Jan 23, 2024 12:00 AM | | 8 | |
| □ | CVE-2024-0519 | High | 8.8 | Microsoft Edge Chromium-based (+ 6... | 9 days | Jan 16, 2024 12:00 AM | Jan 16, 2024 7:41 PM | Jan 23, 2024 12:00 AM | | 8 | |
| □ | CVE-2024-20721 | Medium | 4.0 | Microsoft Edge Chromium-based | 14 days | Jan 11, 2024 8:00 AM | Jan 18, 2024 1:35 AM | Jan 18, 2024 8:00 AM | | 50 | |
| □ | CVE-2024-21337 | Medium | 5.2 | Microsoft Edge Chromium-based | 14 days | Jan 11, 2024 5:00 AM | Jan 12, 2024 1:49 AM | Jan 18, 2024 7:13 PM | | 50 | |
| □ | CVE-2024-20675 | Medium | 6.3 | Microsoft Edge Chromium-based | 14 days | Jan 11, 2024 5:00 AM | Jan 18, 2024 1:47 AM | Jan 18, 2024 7:14 PM | | 50 | |
| □ | CVE-2024-20709 | Low | 3.7 | Microsoft Edge Chromium-based | 15 days | Jan 10, 2024 4:00 PM | Jan 12, 2024 1:49 AM | Jan 18, 2024 8:00 AM | | 50 | |
| □ | CVE-2024-21320 | Medium | 6.5 | Microsoft Windows 10 (+ 6 more) | 16 days | Jan 9, 2024 12:00 AM | Jan 9, 2024 6:30 PM | Jan 12, 2024 5:14 PM | | 283 | |
| □ | CVE-2024-21319 | Medium | 6.8 | Oracle Aspnetcore (+ 41 more) | 16 days | Jan 9, 2024 12:00 AM | Jan 9, 2024 6:30 PM | Jan 16, 2024 8:48 PM | | 13 | |
| □ | CVE-2024-21316 | Medium | 6.1 | Microsoft Windows 10 (+ 4 more) | 16 days | Jan 9, 2024 12:00 AM | Jan 9, 2024 6:30 PM | Jan 12, 2024 6:46 PM | | 279 | |

6. **Event timeline**: Lists vulnerabilities that affect your organization in a timeline view.



Selected device groups (9/9)

### Event timeline

New vulnerabilities 590

Exploitable vulnerabilities 5

Custom range From 4/3/20 To 7/2/20 Search events

| Date (UTC) ↑ | Event | Related component | Originally impacted device... | Currently impacted devices ... | Type |
|---|---|---|---|---|---|
| 4/14/20 | An exploit for 1 vulnerability in Microsoft Windows 7 became verified, currently i... | Microsoft Windows 7 | N/A | 1.04k (<1%) | Exploit was verified |
| 4/14/20 | [redacted] has a new vulnerability, currently impacting 634 devices | Adobe Digital Editions | N/A | 634 (<1%) | New vulnerability |
| 4/14/20 | 1 vulnerability in Microsoft Windows Server 2012 R2 became exploitable, currentl... | Microsoft Windows Server 2012 R2 | N/A | 2.66k (1%) | New public exploit |
| 4/14/20 | An exploit for 1 vulnerability in Microsoft Windows Server 2012 R2 became verifie... | Microsoft Windows Server 2012 R2 | N/A | 2.66k (1%) | Exploit was verified |