

# Get a real-time in-depth view of new and trending CVEs with the Vulnerability Dashboard

Discover trending, weaponized, and exploited vulnerabilities with links to threat actors and malware

February 2024

## Vulnerability Dashboard EXPORT

Filters

📅 Last 24 hours

AND

📈 Trending ✕ + OR 🗑️

+ AND ⋮

SAVE VIEW CLEAR

Total vulnerabilities 🔍

182

Weaponized vulnerabilities 🔍

124

Exploited vulnerabilities 🔍

124

**Most affected vendors and products** See more

● Apple 21% ● Microsoft 18% ● Oracle 14% ● Linux 14% ● IBM 8% ● Other 25%

**Attribution of exploits** See more

● APT 21 25% ● Lazarus Group 19% ● Sea Turtle 16% ● APT35 12% ● Inception Framework 10% ● Other 18%

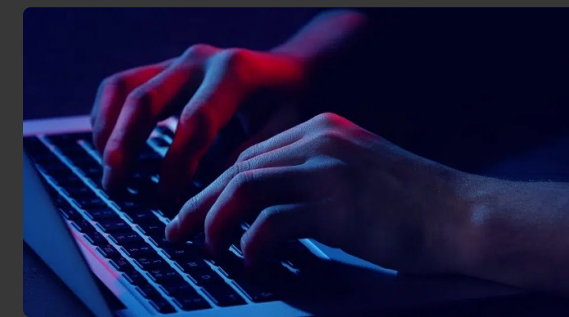
**Vulnerabilities** SHOW/HIDE COLUMNS

CVE ID	CVSS SCORE	VENDORS	TREND	EXPLOIT
<b>CVE-2023-3824</b> <small>In PHP version 8.0.* before 8.0.30, 8.1.* before 8.1.22, and 8.2.* before 8.2.8, when loading phar file, while reading PHAR directory...</small>	CVSS 9.8	Php	 187 articles	02/19/2024
<b>CVE-2024-22245</b> <small>Arbitrary Authentication Relay and Session Hijack vulnerabilities in the deprecated VMware Enhanced Authentication Plug-in (EAP)...</small>	CVSS 9.6	VMWare	 13 articles	-
<b>CVE-2024-21410</b> <small>Microsoft Exchange Server Elevation of Privilege Vulnerability</small>	CVSS 9.7	Microsoft	 320 articles	02/15/2024
<b>CVE-2023-50387</b> <small>Certain DNSSEC aspects of the DNS protocol (in RFC 4035 and related RFCs) allow remote attackers to cause a denial of service ...</small>	CVSS 7.5	Redhat	 260 articles	14/11/2023

“

**Discovering and researching vulnerabilities is a very complex and timely process due to the large volume and available technologies**

Director of information Security, Financial Institution



Lace Tempest hackers behind active exploitation of MOVEit

Proof of Exploit



in TrueBot with new

# Discover new and trending CVEs with the Vulnerability Dashboard

- In-depth real-time CVE table
- Customizable to your intelligence needs
- Key overview metrics
- PDF Export

## Vulnerability Dashboard

EXPORT

Filters

Last 24 hours

AND

Trending + OR

+ AND

SAVE VIEW

CLEAR

Total vulnerabilities ⓘ

182

Weaponized vulnerabilities ⓘ

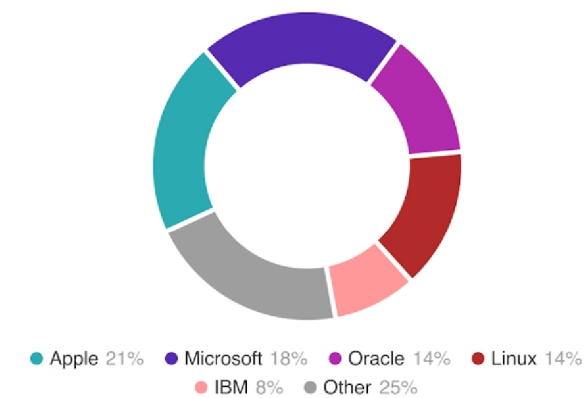
124

Exploited vulnerabilities ⓘ

124

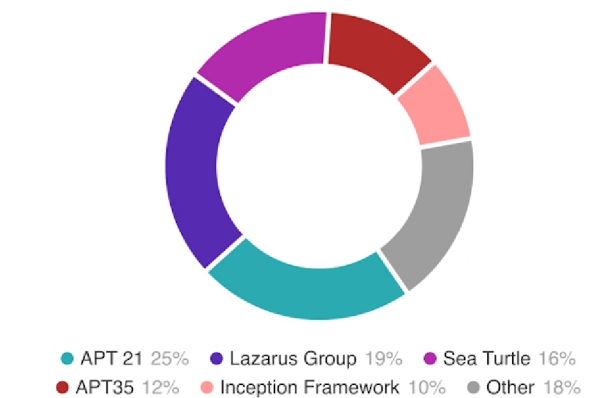
Most affected vendors and products

See more



Attribution of exploits

See more



### Vulnerabilities

SHOW/HIDE COLUMNS

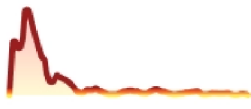
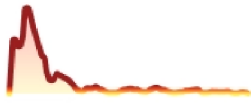
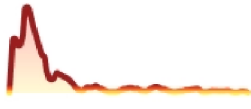
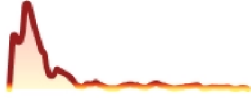
CVE ID	CVSS SCORE	VENDORS	TREND	EXPLOIT
<b>CVE-2023-3824</b> In PHP version 8.0.* before 8.0.30, 8.1.* before 8.1.22, and 8.2.* before 8.2.8, when loading phar file, while reading PHAR directory...	CVSS 9.8	Php	 187 articles	02/19/2024
<b>CVE-2024-22245</b> Arbitrary Authentication Relay and Session Hijack vulnerabilities in the deprecated VMware Enhanced Authentication Plug-in (EAP)...	CVSS 9.6	VMWare	 13 articles	-
<b>CVE-2024-21410</b>	CVSS 9.7	Microsoft		02/15/2024

# In-depth real-time CVE table

Get an in-depth view of new and trending CVEs. Extracted and enriched by Feedly AI in real-time.

### Vulnerabilities

SHOW/HIDE COLUMNS

CVE ID	CVSS SCORE	VENDORS	TREND	EXP
<b>CVE-2022-21874</b> Windows Security Center API Remote Code Execution Vulnerability.	CVSS 10	Microsoft	 14 articles	14/
<b>CVE-2022-21874</b> DirectX Graphics Kernel Remote Code Execution Vulnerability. This CVE ID is unique from CVE-2022-21912.	CVSS 9.8	Google	 14 articles	14/
<b>CVE-2022-21874</b> Windows Security Center API Remote Code Execution Vulnerability.	CVSS 9.7	Apple +5 others	 14 articles	14/
<b>CVE-2022-21874</b> Windows Security Center API Remote Code Execution Vulnerability.	CVSS 6.3	Microsoft	 14 articles	14/

SHOWN

- CVE ID
- CVSS
- Vendors
- Trend
- Exploit
- Malware

HIDDEN

- CISA KEV
- Threat Actors
- Published Date
- EPSS

# Customizable to your specific vulnerability intelligence needs

Save searches to ensure quick access to the latest updates and continuous monitoring

## Vulnerability Dashboard

EXPORT

Filters

Last 24 hours

AND

Trending + OR

+ AND

SAVE SEARCH

Total vulnerabilities

182

Most affected vendors

Apple 32%

Search

- Exploited
- Weaponized
- CISA KEV
- Latest vulnerabilities detected by scanners
- CVE IDs
- Threat Actors
- Malware Families
- Vendors
- CVSS
- CVSS Estimate
- Attack Vector

Exploited vulnerabilities

Exploited vulnerabilities

124

Attribution of exploits

See more



APT 21 32% Lazarus Group 32% Sea Turtle 32% APT35 32% Inception Framework 32% Other 32%

Total vulnerabilities ⓘ

182

Weaponized vulnerabilities ⓘ

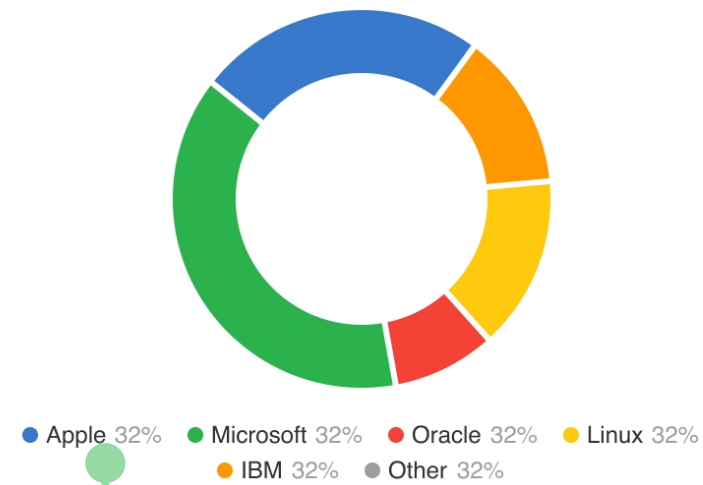
124

Exploited vulnerabilities ⓘ

124

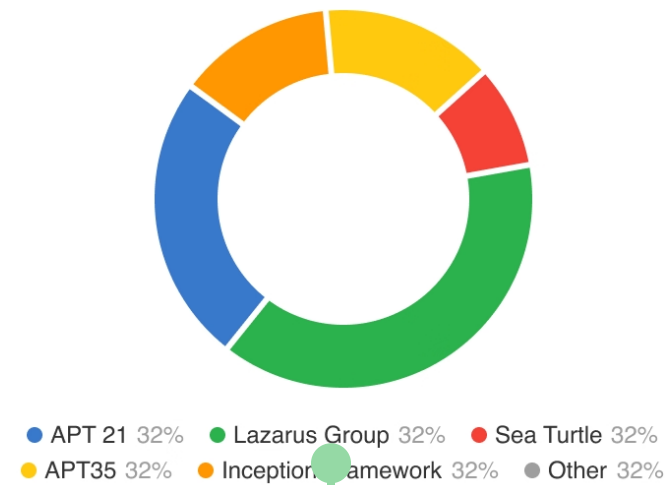
### Most affected vendors and products

[See more](#)



### Attribution of exploits

[See more](#)



# Gain a real-time overview of the vulnerability landscape

- Discover the most vulnerable vendors
- Links to threat actors and malware

## Apple

CVE ID	CVSS	EXPLOIT	PATCH	TRENDS
<b>CVE-2024-23224</b> The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.3, macOS Ventura 13.6.4. An app may b...	CVSS 5.5	-	Patched	
<b>CVE-2024-23223</b> A privacy issue was addressed with improved handling of files. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, tvOS 17.3, iO...	CVSS 6.2	-	Patched	
<b>CVE-2024-23222</b> A type confusion issue was addressed with improved checks. This issue is fixed in iOS 17.3, iOS 17.3 and iPadOS 17.3, macOS...	CVSS 8.8	Exploit	Patched	
<b>CVE-2024-23219</b> The issue was addressed with improved authentication. Stolen Device Protection may be unexpectedly disabled	CVSS 6.2	-	Patched	
<b>CVE-2024-23218</b> A timing side-channel issue was addressed with improvements to constant-time computation in cryptographic functions. An...	CVSS 5.9	-	Patched	
<b>CVE-2024-23217</b> A privacy issue was addressed with improved handling of temporary files. This issue is fixed in macOS Sonoma 14.3, watchOS 10.3, iO...	CVSS 3.3	-	Patched	
<b>CVE-2024-23215</b> An issue was addressed with improved	CVSS 5.5	-	Patched	

Beta

THREAT ACTOR FROM NORTH KOREA 🇰🇷

## Lazarus Group

17 mentions in the last 2 weeks

3K articles in the last 12 months

ⓘ Using open-source data collected by Feedly AI.

#### Overview

Since 2009, HIDDEN COBRA actors have leveraged their capabilities to target and compromise a range of victims; some intrusions have resulted in the exfiltration of data while others have been disruptive in nature. Commercial reporting has referred to this activity as Lazarus Group and Guardians of Peace. Tools and capabilities used by HIDDEN COBRA actors include DDoS botnets, keyloggers, remote ac... [See More](#)

#### Aliases

- APT 38
- APT-C-26
- ATK 117
- ATK 3

[See 35 more aliases](#)

#### Targets

- Australia
- Bangladesh
- Bangladesh Bank