

# Most Critical Vulnerability Insights

Quarterly Vulnerability Report,  
April to June Edition 2022

2022



# Q2 Vulnerability Report

We have crossed the halfway mark of 2022, and the first six months of the year have already witnessed a wide range of vulnerabilities. **According to SecPod's security research, the second quarter of 2022 saw a total of 5478 vulnerabilities with 7 zero days.** Although the number is slightly lesser than the last quarter, there is no doubt it is still a large sum. To stay on top of attacks and boost your cyber defense skills, it is necessary to be aware of the latest vulnerability trends. With broader insights on the top critical vulnerabilities, you can battle out the higher risks faster and reduce the risk exposure in your IT network to a larger extent.

As we always do at SecPod, keeping you equipped with the latest information on vulnerabilities, we have put together the following report covering the insights on vulnerabilities between April and June 2022. The report details the latest vulnerabilities trends and the top critical vulnerabilities discovered in the second quarter of 2022. We recommend you remediate these high-risk vulnerabilities immediately in your network to stay a step ahead of attackers and prevent threatening security mishaps. Let us uncover what was in the vulnerability store from April to June 2022.



# What the report consists of?

The reports consist of the important details of the vulnerabilities that were discovered in from April to June 2022. The vulnerability details are researched and mentioned in the report based on the publish date. You will find detailed insights on the following:

1. Key Findings from SecPod’s Security Research Team	.....	04
2. Total number of vulnerabilities	.....	05
3. Vulnerability Distribution based on CVSS v2 Algorithm, Exploitability Score, and Impact score	.....	06
4. Vulnerability Distribution based on CVSS v3 Algorithm, Exploitability Score, and Impact score	.....	07
5. Top 10 Affected Vendors/Products	.....	08
6. Top 10 Affected Operating systems	.....	09
7. Top 10 Affected Applications	.....	09
8. Top 10 Affected Hardware	.....	09
9. Top 10 Most Critical Vulnerabilities	.....	10
10. Zero Day Vulnerabilities Discovered Between April and June 2022	.....	11
11. Analytics of Malware Vulnerability Enumeration (MVE)	.....	13
12. Vulnerability Prediction of the upcoming months using the ARIMA model	.....	14
13. SecPod’s Security Intelligence Coverage from April to June 2022	.....	14



2022



# Key Findings from SecPod's Security Research Team

**5478** is the **number of vulnerabilities discovered** between April and June 2022, which is **13.7 %** less than the first three months of 2022.

As per **CVSS v3**, **3096** vulnerabilities were reported with **critical & high severity in the second quarter of 2022, 6.7 % less** than the first three months of 2022.

As per **the CVSS v2** algorithm, **1362** vulnerabilities were reported with **critical and high severity in the second quarter of 2022, 5.8% less** than the first quarter of 2022.

**7 zero days** were discovered in the first three months of 2022.

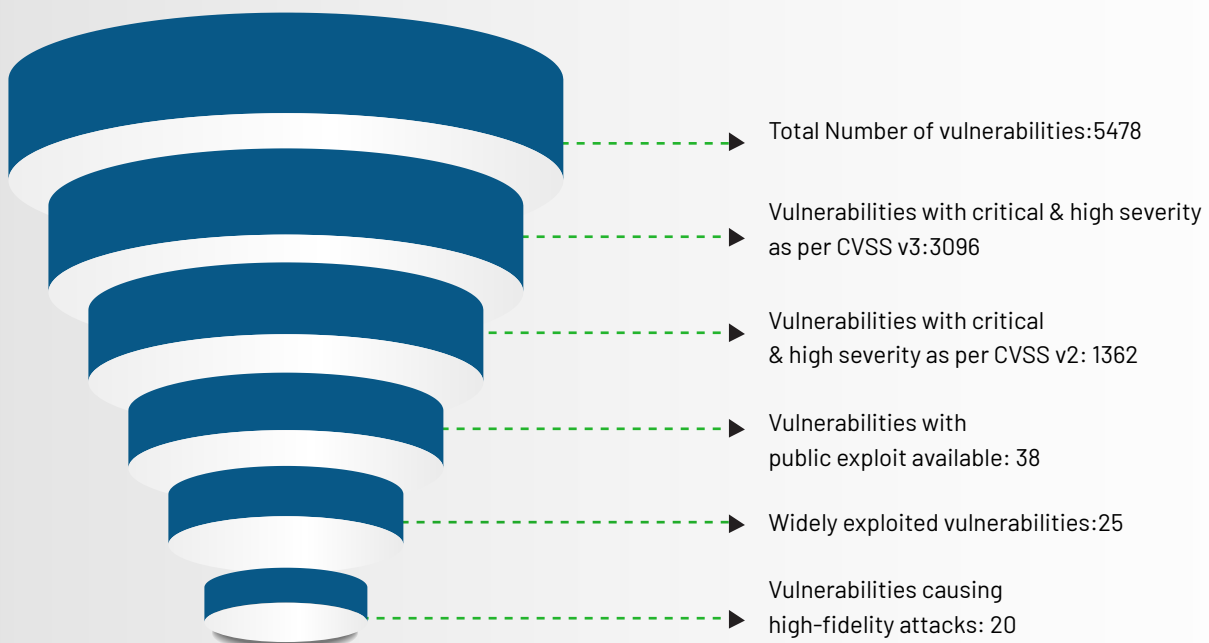
**25** of the total vulnerabilities discovered are **widely exploited**.

**20** of the total vulnerabilities have **public exploits** available.

**20** of the total vulnerabilities discovered causes **High-fidelity attacks** and are **Malware Exploiting Vulnerabilities**

**61 web browser vulnerabilities** were discovered in the second quarter of 2022.

## Vulnerability Trend – Q2, 2022



## SecPod's Security Intelligence Coverage in April to June 2022

- Total No of CVEs Covered: 6717
- No of Local Checks: 6632
- No of Remote Checks: 85
- Zero-day CVEs covered: 15

CVEs based on platforms:

- Windows - 663
- Unix - 1651
- macOS - 382

- 
- CISA Vulnerabilities Coverage: **669/789**
  - Network Device Vulnerabilities: **1025**
  - Total No of Misconfigurations covered: **1625**
  - Total No of Third-party applications Patches Covered: **201**
  - To No of Misconfigurations patches covered: **1479**
  - Total No of OS Patches Covered: **All latest Versions for the Supported OS**

1 1 0 1 0 1

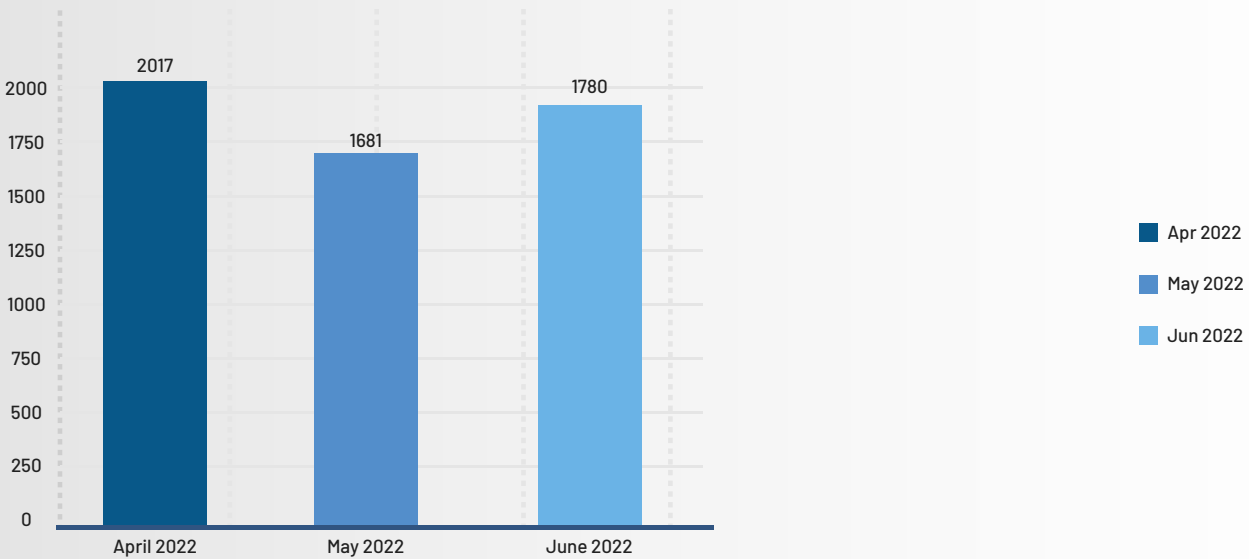
1 1 0 1 0 0 0 1 1 0 1 0 1



# Total Number of CVEs discovered

Figure 1: Shows the number of vulnerabilities published from April to June 2022.

NUMBER OF VULNERABILITIES PUBLISHED IN Q2 2022

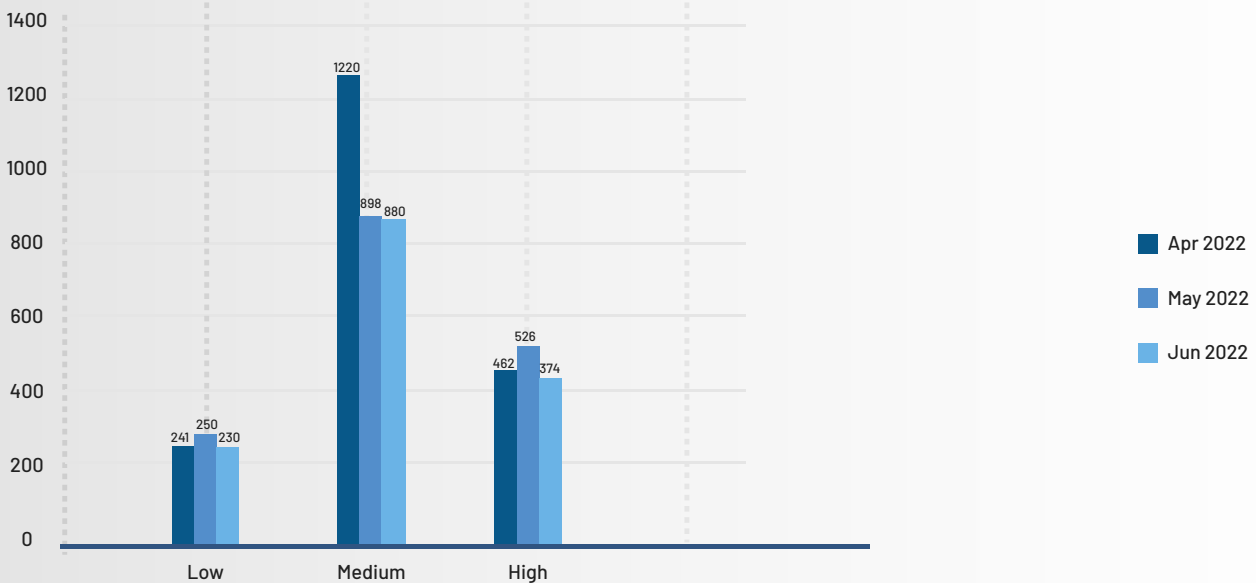


The number of vulnerabilities published in the second quarter of 2022 is 5478, 13.7% less than the 6309 vulnerabilities published in the first three months of 2022. This list includes a total of 7 zero-day vulnerabilities.

## Vulnerability Severity Distribution based on CVSS v2:

Figure 2: Depicts the vulnerability severity distribution based on the CVSS v2 algorithm.

VULNERABILITIES PUBLISHED IN Q2 2022



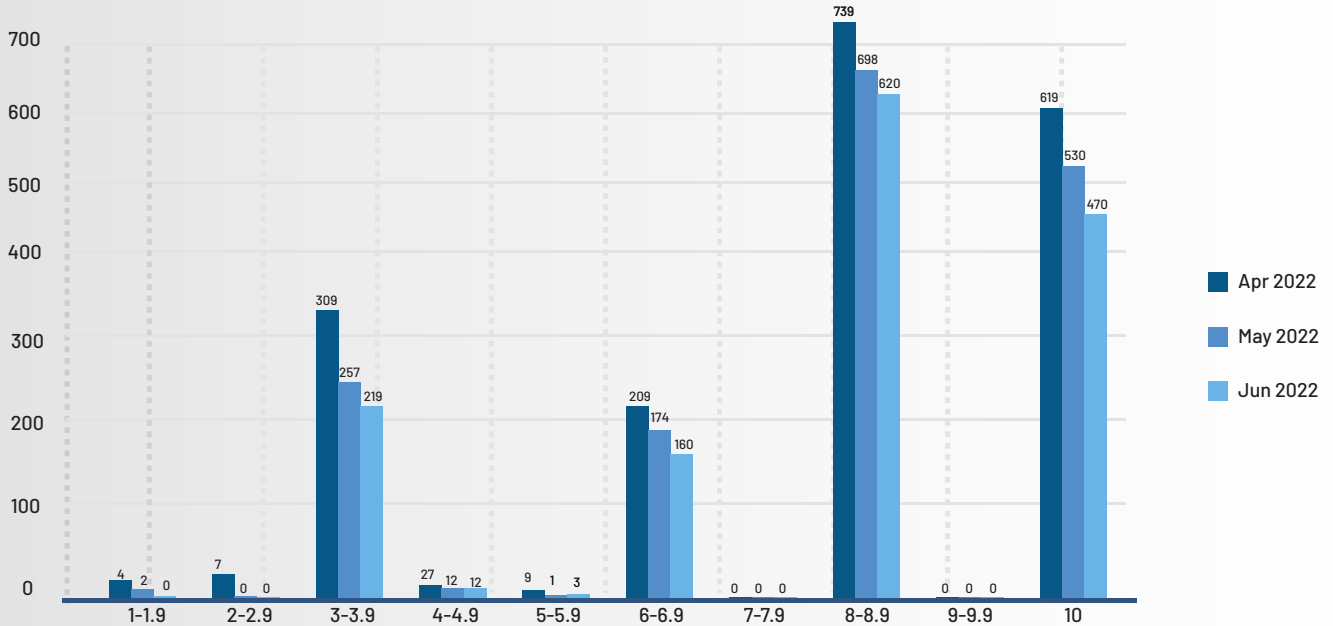
As per the CVSS v2 algorithm, 721 vulnerabilities were reported with low severity, 2998 vulnerabilities were reported with a medium severity, and 1362 vulnerabilities were reported with high severity



# Vulnerability Distribution based on CVSS v2 Exploitability Score

Figure 3: Depicts the distribution of vulnerabilities based on CVSS v2 exploitability score.

CVSSV2 EXPLOITABILITY SCORE OF VULNERABILITIES THAT APPEARED IN Q2 2022

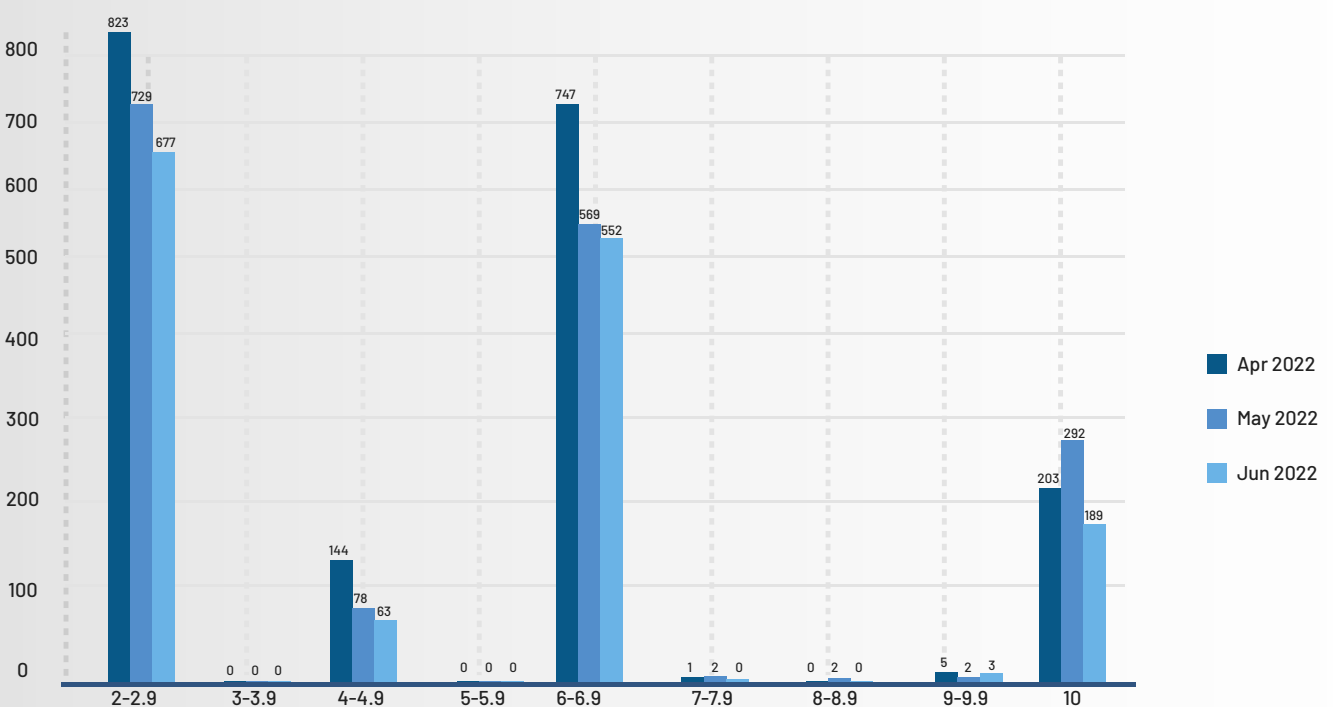


More vulnerabilities fall in the exploitability score of 8 – 8.9, followed by the exploitability score of 10. The maximum number of vulnerabilities falls in the range above 8, and this is critical.

# Vulnerability Severity Distribution based on CVSS v2 Impact Score

Figure 4: Depicts the distribution of vulnerabilities based on CVSSv2 impact score.

CVSSV2 IMPACT SCORE OF VULNERABILITIES THAT APPEARED IN Q2 2022

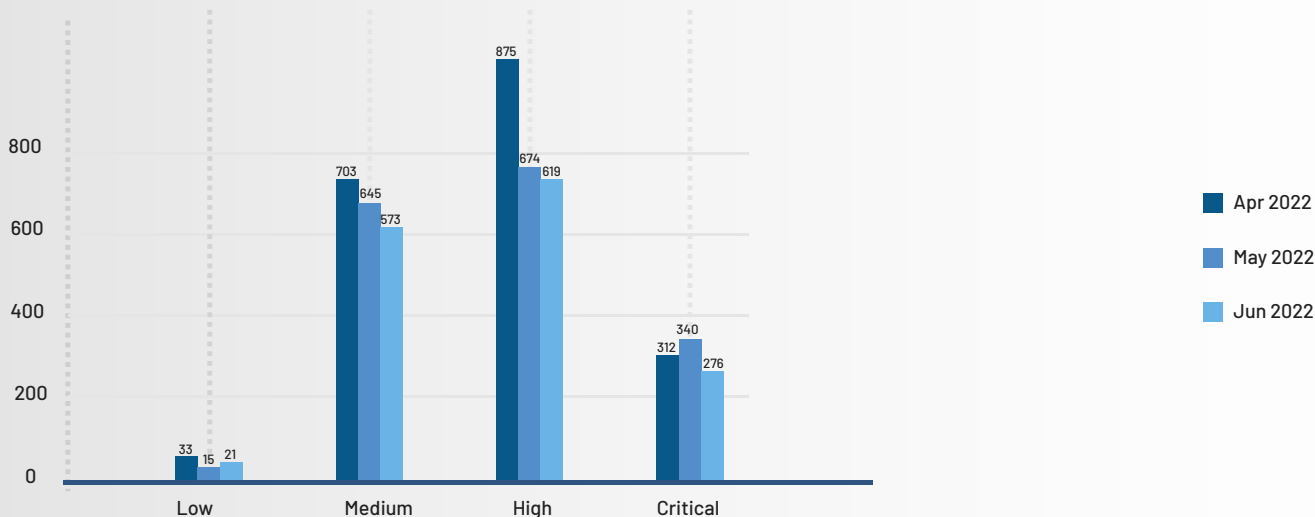


More than 600 vulnerabilities lie in the maximum impact score of 10.

# Vulnerability Severity Distribution based on CVSS v3

Figure 5: Depicts the vulnerability severity distribution based on CVSS v3.

VULNERABILITIES PUBLISHED IN 2022 Q2, ACCORDING TO THEIR CVSSV3 BASE SCORE

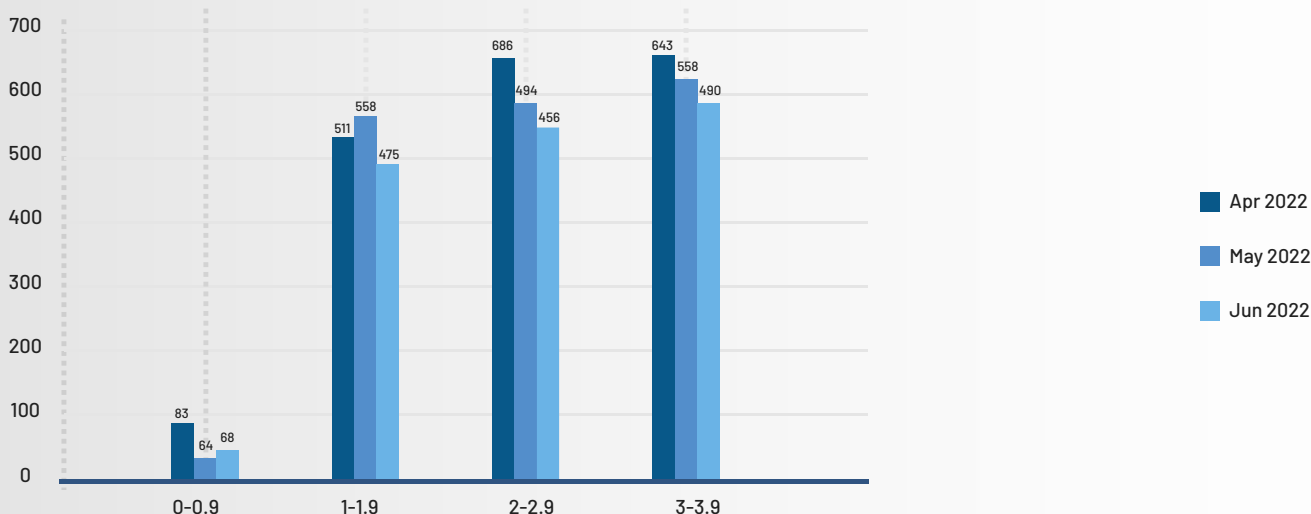


As per CVSS v3 score, 69 vulnerabilities were reported with low severity, 1921 vulnerabilities were reported with medium severity, 2168 vulnerabilities were reported with high severity, and 928 vulnerabilities were reported critical.

# Vulnerability Severity Distribution based on CVSS v3 Exploitability Score

Figure 6: Depicts the distribution of vulnerabilities based on the exploitability score of CVSS v3.

CVSSV3 EXPLOITABILITY SCORE OF VULNERABILITIES THAT APPEARED IN Q2 2022



More vulnerabilities are reported in the range of 2-2.9 and 3-3.9 exploitability scores.

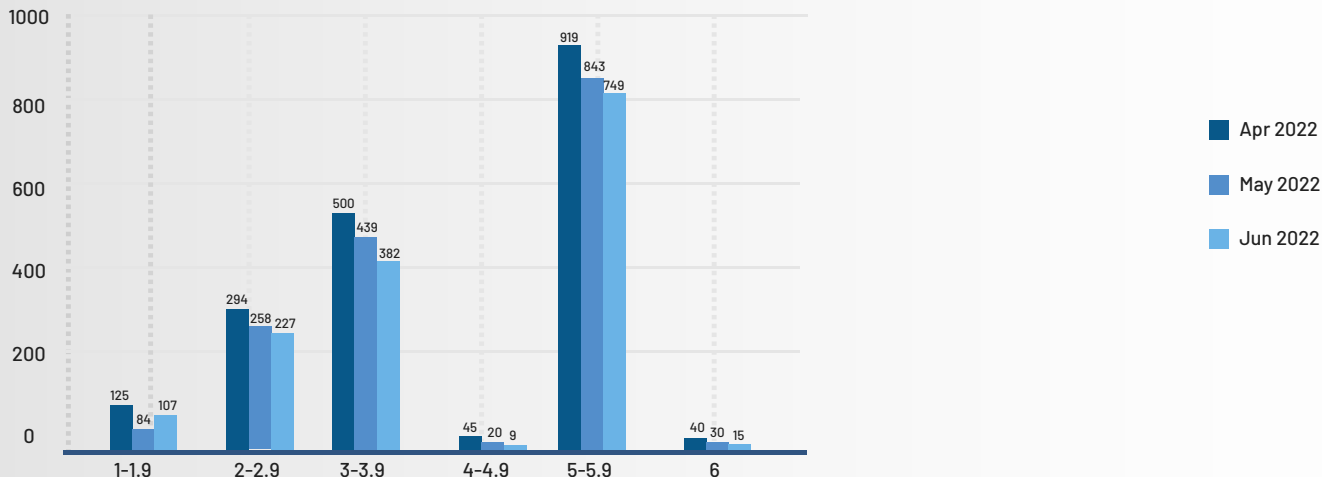




# Vulnerability Severity Distribution based on CVSS v3 Impact Score

Figure 7: Depicts the distribution of vulnerabilities based on the impact score of CVSS v3.

CVSSV3 IMPACT SCORE OF VULNERABILITIES THAT APPEARED IN Q2 2022

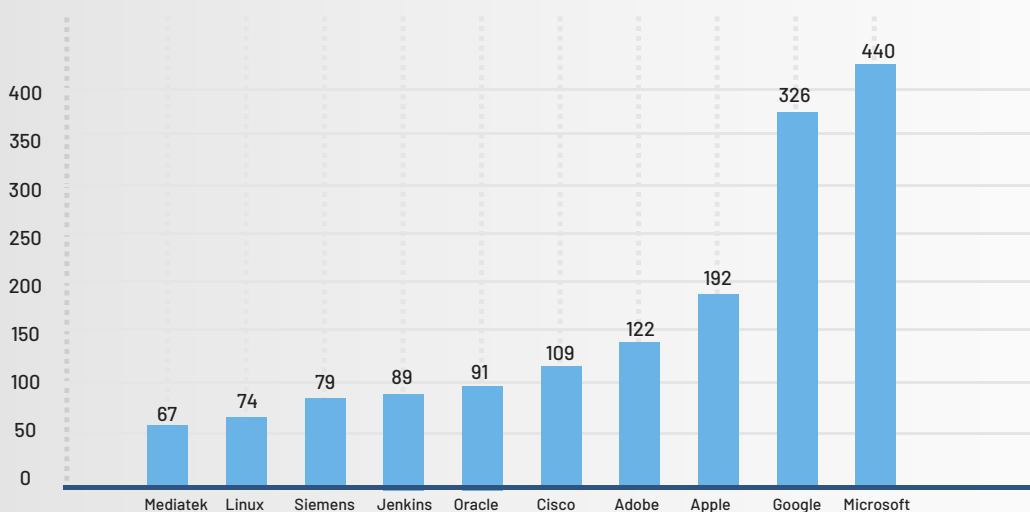


More Vulnerabilities are falling in the impact score range between 5 to 5.9.

## Top 10 Affected Vendors/Products

Figure 8: Shows the Top 10 vendors affected by CVEs.

TOP 10 VENDORS AFFECTED BY CVEs



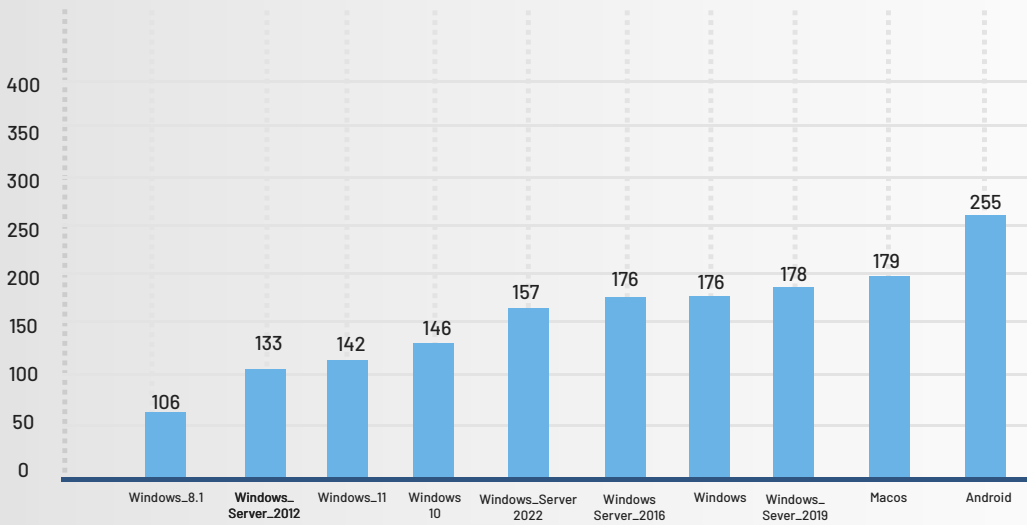
Microsoft and Google are the most affected Vendors in the second quarter of 2022. Respectively they have reported 440 and 326 vulnerabilities each.



# Top 10 Affected Operating Systems

Figure 9: Shows the Top 10 Operating Systems Affected by CVEs.

TOP 10 OS AFFECTED BY CVEs

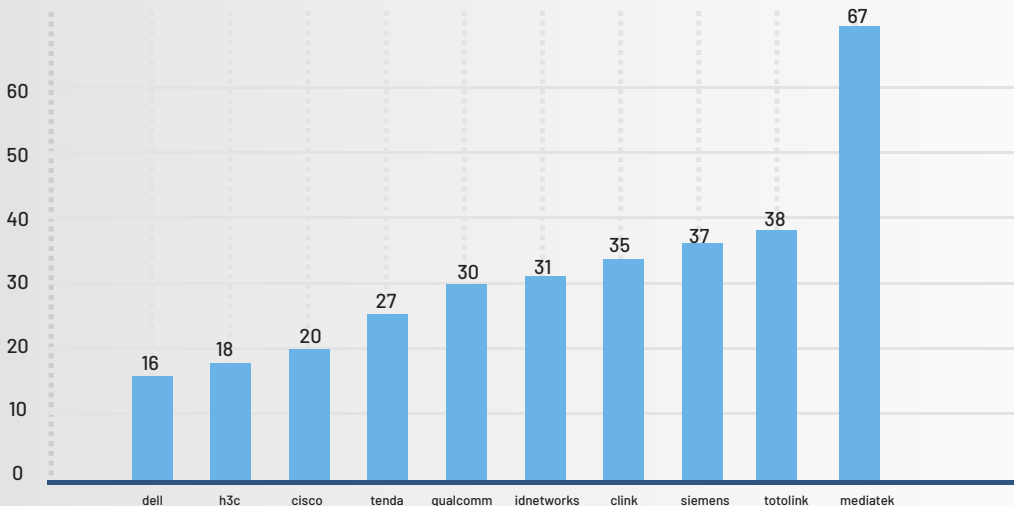


Android is the most affected operating system, with a total of 255 vulnerabilities. Mac and Windows operating systems also report a fair share of vulnerabilities. Linux operating system is not present in the top 10 list of 2022's second quarter.

# Top 10 Affected Hardware

Figure 10: Shows the Top 10 Hardware Affected by CVEs.

TOP 10 AFFECTED HARDWARE




Rlc-410w has reported the highest number of vulnerabilities in the first three months of 2022. It has reported over 79 vulnerabilities in this quarter.



# Top 10 Most Critical Vulnerabilities

This section provides the details of the Top 10 most critical vulnerabilities discovered between April and June 2022. The information on the vulnerabilities includes the CVE details, CVSS number, the affected products, and the impact of the vulnerability. We recommend you to immediately identify and remediate these vulnerabilities in your network to prevent potential attacks.

S.No	CVE ID	Affected Products	CVSS	Impact
1	CVE-2022-24086	 Adobe Commerce and Magento Open Source	9.8	Arbitrary code execution
2	CVE-2022-1040	 Sophos Firewall	9.8	Arbitrary code execution
3	CVE-2022-26937	 Windows	9.8	Remote code execution, unsuccessful exploitation could crash the system
4	CVE-2022-1364	 Google Chrome, Microsoft Edge Chromium	8.8	Engine crashes and browser might become unresponsive
5	CVE-2021-31805	 Apache Struts	9.8	Remote code execution
6	CVE-2022-30190	 Windows	7.8	Arbitrary Code Execution
7	CVE-2022-30136	 Windows	9.8	Remote code execution and unsuccessful exploitation could crash the system
8	CVE-2022-26134	 Confluence Server and Confluence Data Center	9.8	Deploy any backdoor, ransomware, information stealer, and RATs desired and lead a high alert campaign against organizations using these mentioned products



9	CVE-2022-0540	 Jira Core Server Jira Software Server Jira Software Data Center Jira Service Management Server Jira Service Management Data Center	9.8	Authentication Bypass
10	CVE-2022-29464	 WSO2 API Manager 2.2.0, up to 4.0.0 WSO2 Identity Server 5.2.0, up to 5.11.0 WSO2 Identity Serve Analytics 5.4.0, 5.4.1, 5.5.0, 5.6.0 WSO2 Identity Server as Key Manager 5.3.0, up to 5.11.0 WSO2 Enterprise Integrator 6.2.0, up to 6.6.0 WSO2 Open Banking AM 1.4.0, up to 2.0.0 WSO2 Open Banking KM 1.4.0, up to 2.0.0	9.8	Unrestricted arbitrary file upload, and remote code to execution

Patches are available to remediate all the vulnerabilities mentioned in the table.



# Zero Day Vulnerabilities Discovered Between April and June 2022

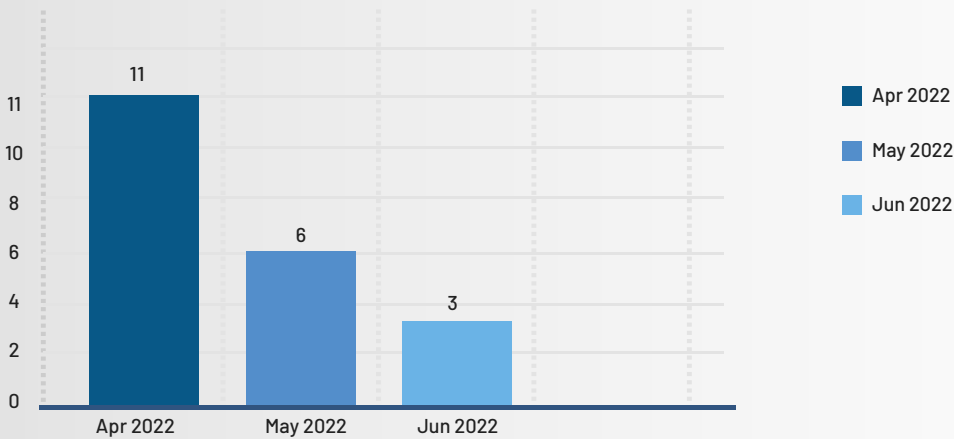
This section consists of the details of the CVEs discovered between April and June 2022. The following 7 zero days were discovered in this quarter.

S.No	CVE ID	Affected Products	Impact	CVSS
1	CVE-2022-30190	 Windows	Remote Code Execution	7.8
2	CVE-2022-26134	 Confluence Server and Confluence Data Center	Deploy any backdoor, ransomware, information stealer, and RATs desired and lead a high alert campaign against organizations using these mentioned products	9.8
3	CVE-2022-26925	 Windows	Unauthenticated attackers can remotely exploit and force domain controllers to authenticate them via the Windows NT LAN Manager (NTLM) security protocol.	8.1
4	CVE-2022-24521	 Windows	Privilege Escalation	7.8
5	CVE-2022-22674	 macOS	Disclosure of Kernel Memory	5.5
6	CVE-2022-22675	 macOS	Arbitrary code execution with Kernel Privileges	7.8
7	CVE-2022-0609	 Google Chrome	Heap Corruption	8.8

# Analysis on High Fidelity Attacks

Figure 11: Depicts the monthly number of vulnerabilities that causes high fidelity attacks.

NO OF HIGH-FIDELITY CVEs IN 2022 Q2

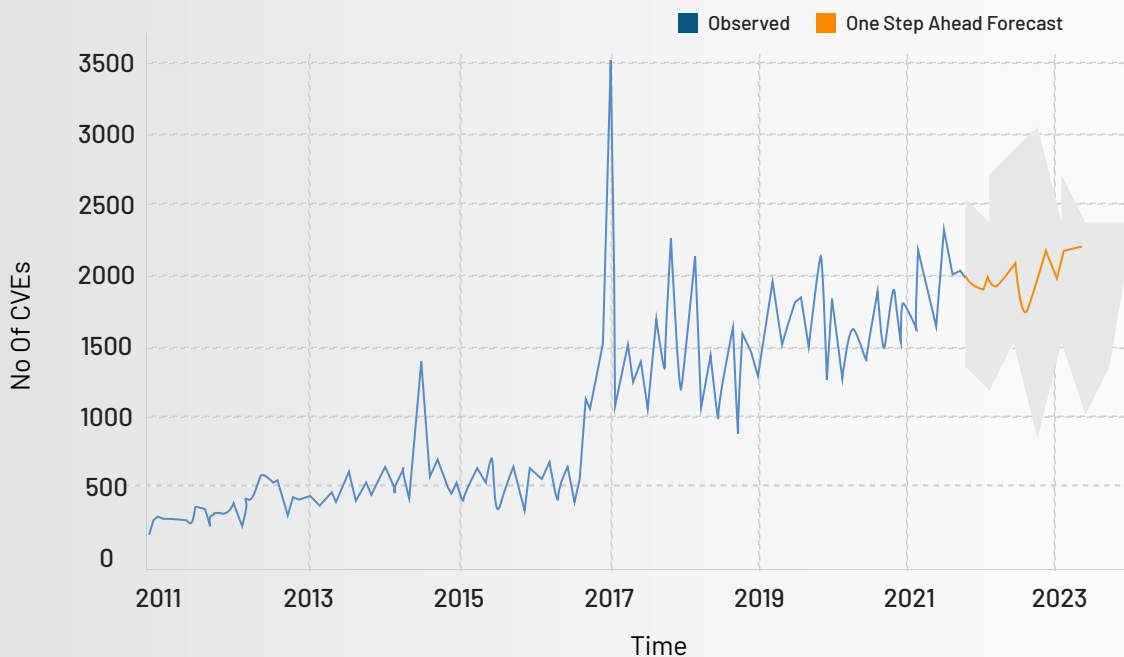


At SecPod, we compare all the discovered CVEs with our researched MVE (Malware Vulnerability Enumeration) data. With this, we identify the vulnerabilities which cause high-fidelity attacks. The number of vulnerabilities that causes high-fidelity attacks is the highest in the month of April. It is highly recommended that these vulnerabilities must be detected and remediated quickly to safeguard your network against cyberattacks.

## Vulnerability Prediction 2022

Figure 12: Displays the Vulnerability trend over the years and predicts the vulnerability count for 2022

FORECASTING NO OF VULNERABILITIES MONTHWISE



On observing the vulnerability trend over the years, from SecPod, we predict over 24000 vulnerabilities in 2022. This prediction is made based on the ARIMA (Autoregressive Integrated Moving Average) model.

# Manage Vulnerabilities and Reduce Risk Exposure with SanerNow Advanced Vulnerability Management

The vulnerabilities count is only going to surge in the days to come, and numerous other security risk exposures also lurk around in the IT landscape. SanerNow Advanced Vulnerability Management provides a continuous and automated solution to manage vulnerabilities, misconfigurations, IT asset exposures, security control deviations, and posture anomalies. Powered by the world's largest security intelligence library with more than 160,000 vulnerability checks, the industry's fastest scans, and integrated patch management, SanerNow detects and remediates vulnerabilities quickly to minimize attack surfaces.

## Experience the Next-gen Vulnerability Management Solution in Action

[Schedule a Demo Now](#)

### About SecPod

SecPod is a cyber security technology company. We prevent cyberattacks. We do everything to prevent attacks on computing environment. Our product helps implement cyber hygiene measures, so attackers have tough time piercing through.

Our SanerNow CyberHygiene platform provides continuous visibility to computing environment, identifies vulnerabilities and misconfigurations, mitigate loopholes to eliminate attack-surface, and helps automate these routines. Our product philosophy is offering simplicity and automation to make the job of security administrators slightly better.



### Contact Us

---

Email us on:

[info@secpod.com](mailto:info@secpod.com)

Call us at:

India - (+91) 80 4121 4020 /

USA - (+1) 918 625 3023

[www.secpod.com](http://www.secpod.com)