

# Most Critical Vulnerability Insights

Quarterly Vulnerability Report,  
July to September Edition 2022

2022



# Q3 Vulnerability Report

We are almost nearing the end of 2022, and the year has already witnessed a total of 17795 vulnerabilities till September 2022. **The third quarter of this year (July to September) saw over 6008 vulnerabilities with 6 zero-days.** The number is rising month on month, and according to the prediction by SecPod's security researchers, we can expect over 24000 vulnerabilities this year. These vulnerabilities, when left unattended, will open gateways for numerous cyberattacks and must be detected and remediation continuously to reduce risk exposure.

To help you to gather detailed insights into the vulnerabilities, SecPod is releasing Quarterly vulnerability reports with details on the vulnerabilities discovered in each quarter. Likewise, we have put together the information on the latest vulnerabilities discovered between July and September 2022 to help you quickly discover and mitigate the vulnerabilities. The report provides details on the top vulnerabilities, zero days, severity details, patch availability status, and numerous trending insights. We recommend you identify and remediate the vulnerabilities discussed in this report to minimize attack surfaces and safeguard your network from potential attacks.

00 011 0101

1 1 01 0 1

1 1 01 0 1 00 011

0101

1 1 01 0 1



# What the report consists of?

The reports consist of the important details of the vulnerabilities that were discovered in from July to September 2022. Note that 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. SecPod’s Security Intelligence Coverage from July to September 2022	.....	05
4. Vulnerability Distribution based on CVSS v3 Algorithm and Exploitability Score	.....	06
5. Top 10 Affected Vendors/Products	.....	06
6. Top 10 Affected Operating systems	.....	08
7. Top 10 Affected Applications	.....	08
8. Top 10 Affected Hardware	.....	09
9. Top 10 Most Critical Vulnerabilities	.....	09
10. Analytics of Malware Vulnerability Enumeration (MVE)	.....	10
11. Vulnerability Prediction of the upcoming months using the ARIMA model	.....	10
		13



2022



# Key Findings from SecPod's Security Research Team

**6008** is the number of vulnerabilities discovered between July and September 2022, **9.6 %** more than the vulnerabilities discovered in second quarter of 2022.

As per **CVSS v3**, **3506** vulnerabilities were reported with **critical & high severity in the third quarter of 2022, 13.2 % less** than the second quarter of 2022.

**6** zero days were discovered in the second quarter of 2022.

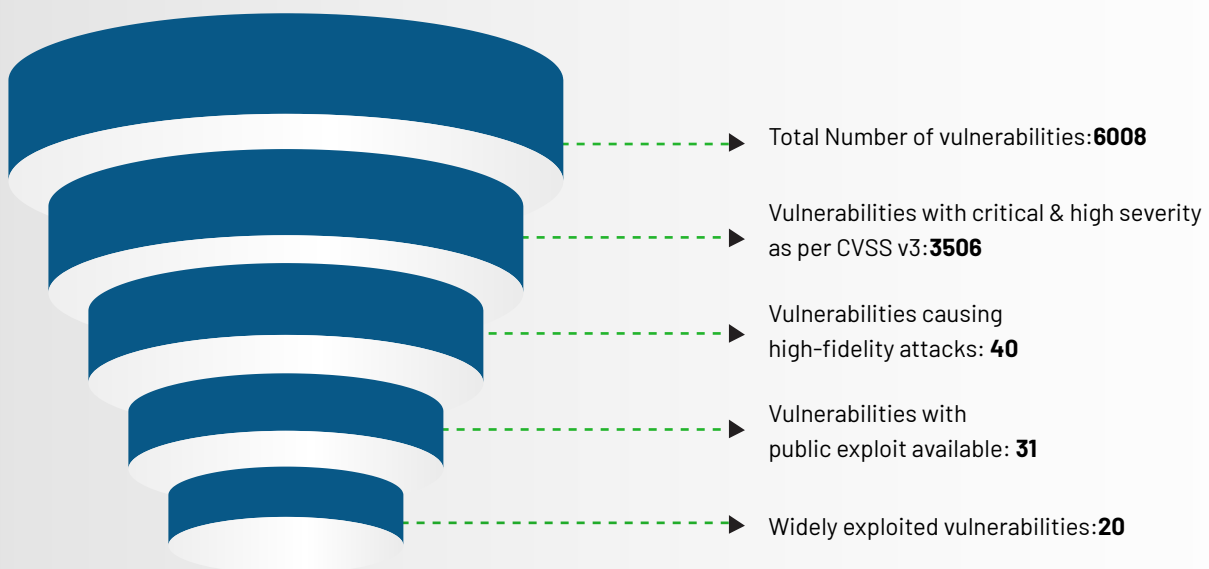
**20** of the total vulnerabilities discovered between July and September 2022 are **widely exploited**.

**31** of the total vulnerabilities discovered in the third quarter of 2022 have **public exploits** available.

**40** of the total vulnerabilities discovered in the third quarter of 2022 are **Malware Exploiting Vulnerabilities**, causing **High-fidelity attacks**

**82 web browser vulnerabilities** were discovered in the third quarter of 2022.

## Vulnerability Trend – Q3, 2022



## SecPod's Security Intelligence Coverage from July to September 2022

### Advanced Vulnerability Coverage

- Total No of CVEs Covered: **5700**
- No of Local Checks (by Saner Agent): **5604**
- No of Remote Checks: **96**
- Zero-day CVEs covered: **6**
- CISA Vulnerabilities Coverage: **764/840**
- Network Device Vulnerabilities: **906**
- Total No of Misconfigurations covered: **2361**
- Total No of Common Configuration Enumeration (CCE) covered: **293**

### CVEs based on Platforms

- Windows - **910**
- Unix - **2065**
- macOS - **363**

### Common Remediation Enumeration (CRE) Coverage

- Total No of Patches Covered: **1152**
- Total No of Third-party applications Patches Covered: **175**
- Total No of Misconfigurations patches covered: **976**
- Total No of OS Patches Covered: **All latest Versions for the Supported OS**

### Compliance Benchmark Coverage Between July and August

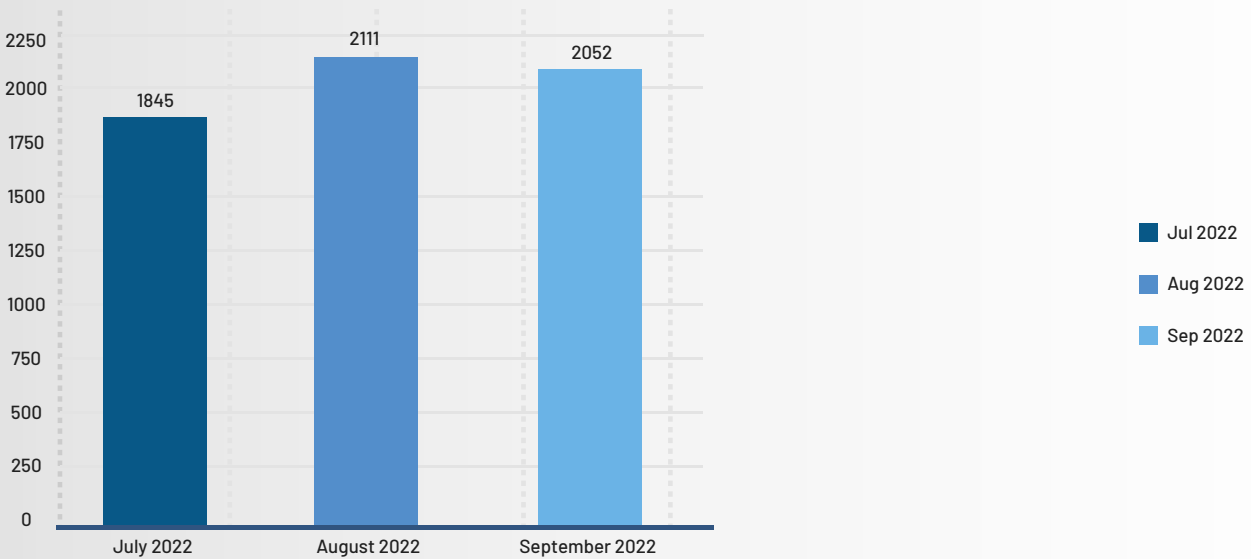
- Microsoft Windows Server 2019 NIST 800-171
- Microsoft Windows 11 NIST 800-53
- Microsoft Windows 11 NIST 800-171
- Microsoft Windows 11 HIPAA
- SUSE Linux Enterprise Server (SLES) 15
- Red Hat Enterprise Linux 9



# Total Number of CVEs discovered

Figure 1: Shows the Number of vulnerabilities published from July to September 2022.

NUMBER OF VULNERABILITIES PUBLISHED IN Q3 2022

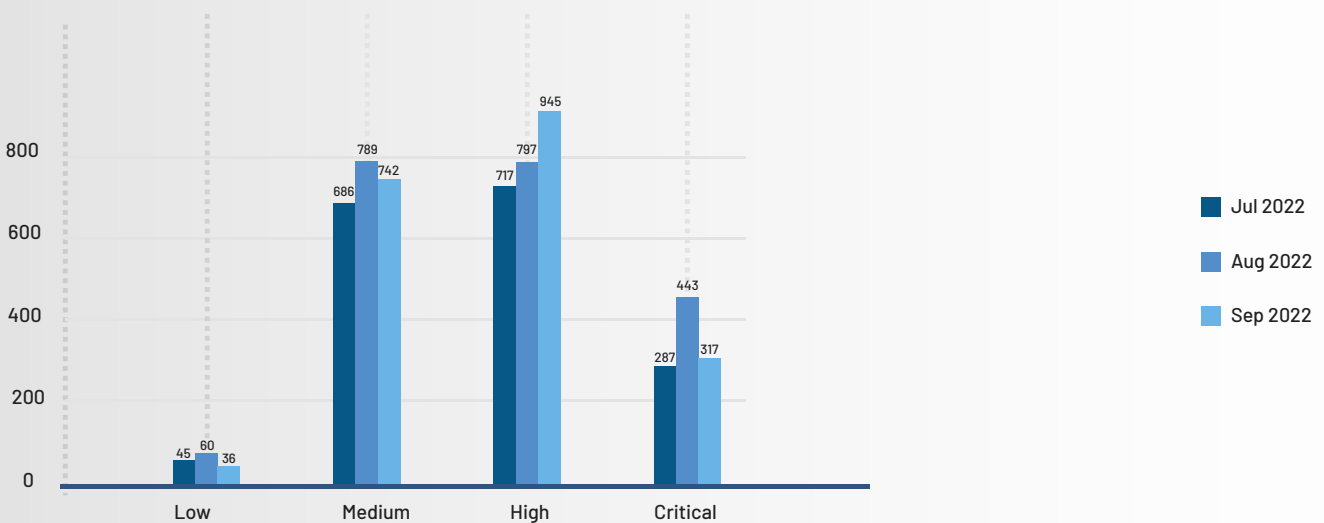


The number of vulnerabilities published in the third quarter of 2022 is 6008, 9.6% more than the 5478 vulnerabilities published in the first three months of 2022. This list includes a total of 8 zero-day vulnerabilities.

## Vulnerability Severity Distribution based on CVSS v3

Figure 2: Depicts the vulnerability severity distribution based on CVSS v3.

VULNERABILITIES PUBLISHED IN Q3 2022

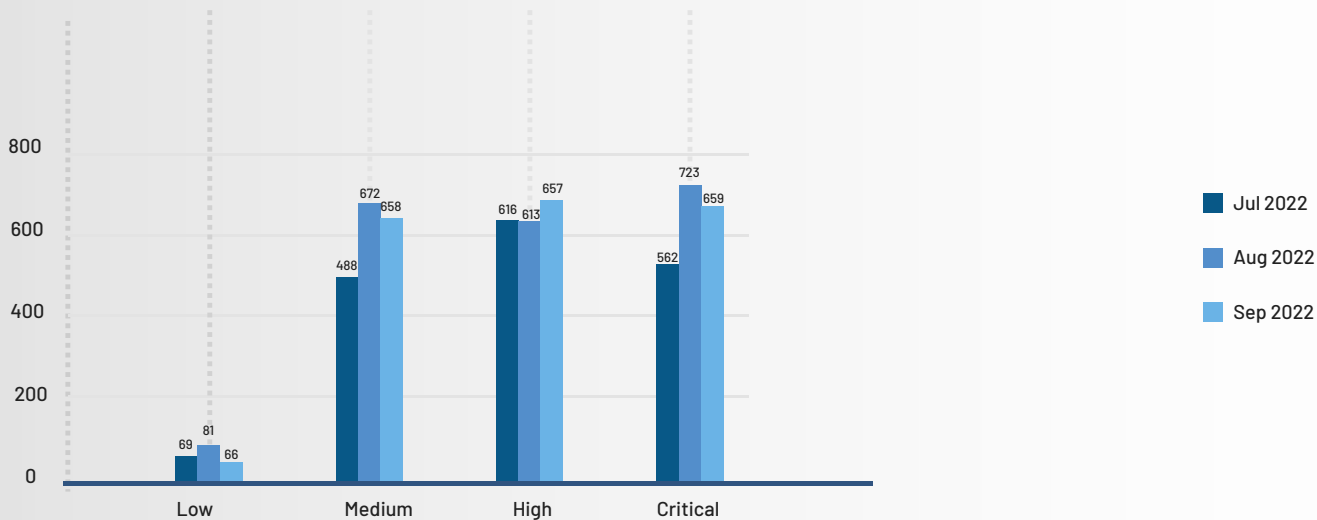


As per the CVSS v3 score, 1047 vulnerabilities are reported with critical severity, and 2459 vulnerabilities are reported with high severity. We can infer that more than 50% of the vulnerabilities discovered in this quarter belong to critical and high severity, which is alarming.

# Vulnerability Severity Distribution based on CVSS v3 Exploitability Score

Figure 3: Depicts the distribution of vulnerabilities based on the exploitability score of CVSS v3

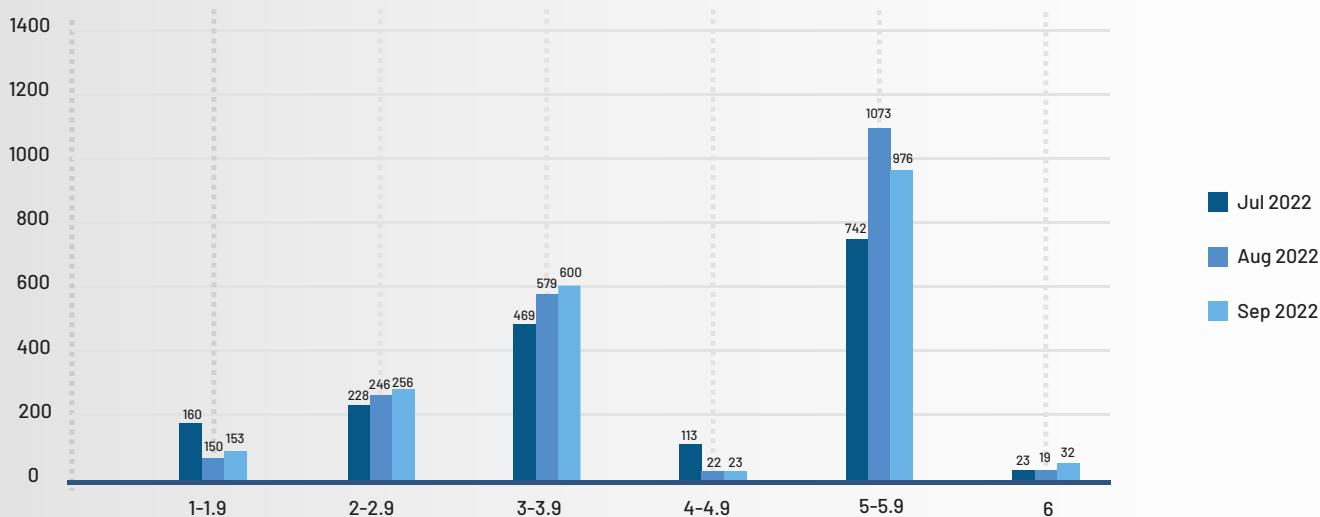
VULNERABILITIES PUBLISHED IN 2022 Q3, ACCORDING TO THEIR CVSSV3 BASE SCORE



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

Figure 4: Depicts the distribution of vulnerabilities based on the impact score of CVSS v3

CVSSV3 EXPLOITABILITY SCORE OF VULNERABILITIES THAT APPEARED IN Q3 2022



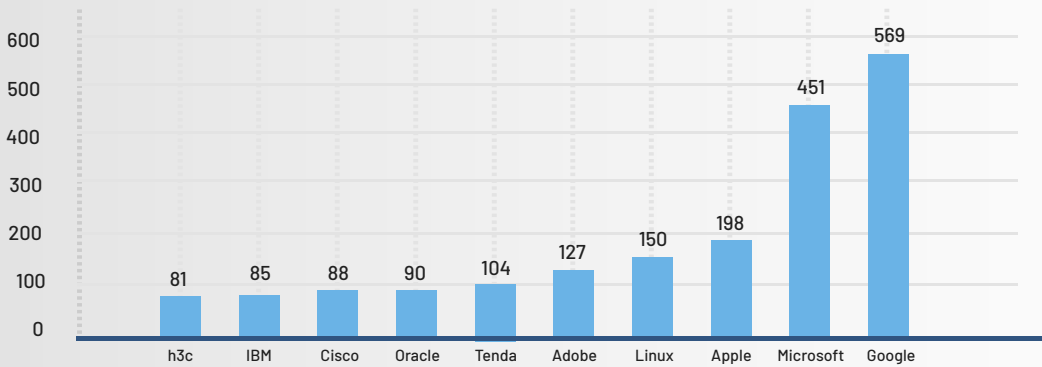
More Vulnerabilities are falling in the impact score range between 5 to 5.9.



# Top 10 Affected Vendors/Products

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

TOP 10 VENDORS AFFECTED BY CVEs

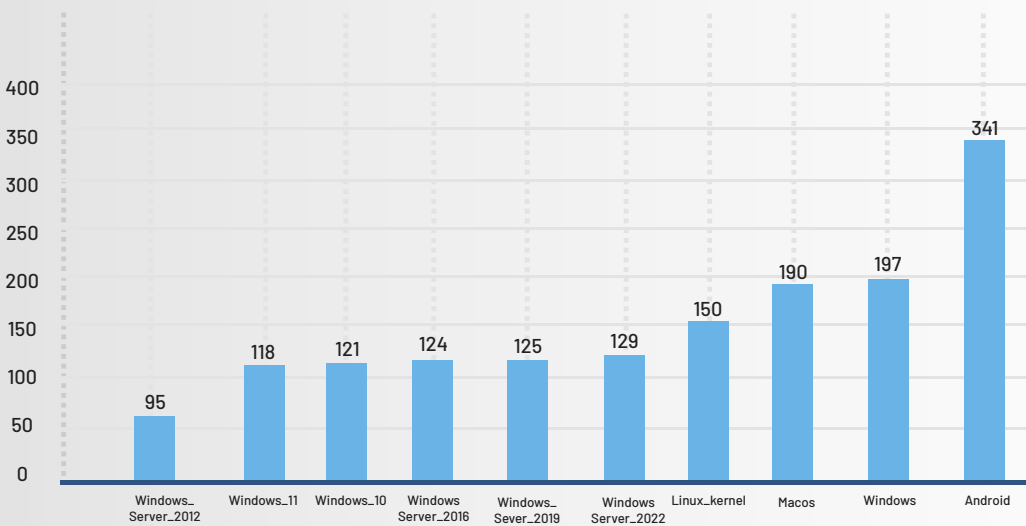


Microsoft and Google are the most affected Vendors in the third quarter of 2022. Respectively they have reported 569 and 451 vulnerabilities each.

# 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 341 vulnerabilities. Windows operating systems also report a fair share of vulnerabilities.

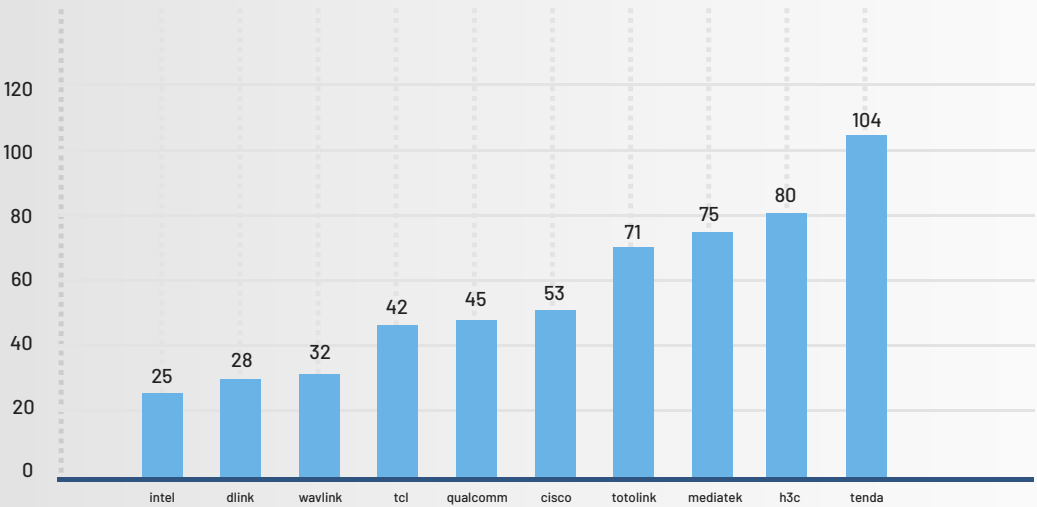




# Top 10 Affected Hardware

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

TOP 10 AFFECTED HARDWARE



Tenda has reported the highest number of vulnerabilities in the third quarter of 2022. It has reported over 104 vulnerabilities, followed by h3c with 80 vulnerabilities.



# Top 10 Most Critical Vulnerabilities

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

S.No	CVE ID	Affected Products	CVSS	Impact
1	CVE-2022-22047	Windows	7.8	Privilege escalation
2	CVE-2022-2274	OpenSSL	9.8	Remote Code Execution
3	CVE-2022-26136 CVE-2022-26137	Bamboo Server and Data Center  Bitbucket Server and Data Center  Confluence Server and Data Center  Crowd Server and Data Center  Fisheye and Crucible  Jira Server and Data Center  Jira Service Management Server and Data Center	9.8	Multiple version ranges
4	CVE-2022-2294	Google Chrome	8.8	Heap Corruption









5	CVE-2022-33891	Apache Struts	8.8	Remote code execution
6	CVE-2022-31676	VMware tools	7	Local privilege escalation
7	CVE-2022-37969	Windows	7.8	Privilege escalation
8	CVE-2022-32917	Apple Mac OS	7.8	Remote code execution
9	CVE-2022-28958 CVE-2022-26258	D-Link Routers	9.8	Remote code execution
10	CVE-2022-41040 CVE-2022-41082	Microsoft Exchange Server	8.8	Remote code execution

Patches are available to remediate all the vulnerabilities mentioned in the table except for CVE-2022-41040 & CVE-2022-41082.



# Zero Day Vulnerabilities Discovered Between July and September 2022

This section consists of the details of the CVEs discovered between July and September 2022. The following 6 zero days were discovered in this quarter.

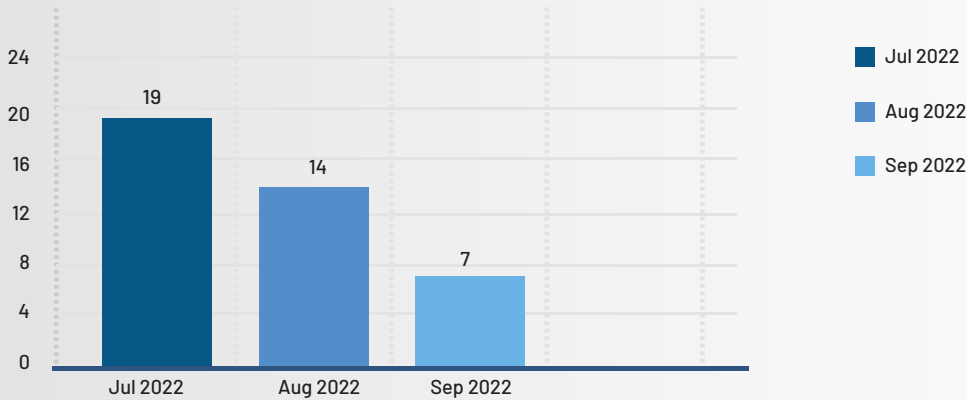
S.No	CVE ID	Affected Products	Impact	CVSS
1	CVE-2022-22047	 Windows	Privilege Escalation	7.8
2	CVE-2022-2294	 Google Chrome	Heap Corruption	9.8
3	CVE-2022-32917	 macOS	Remote code execution	8.1
4	CVE-2022-2856	 Windows	Remote Code Execution	7.8
5	CVE-2022-32894	 macOS	Remote Code Execution	5.5
6	CVE-2022-32893	 macOS	Remote Code Execution	7.8



# 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 Q3

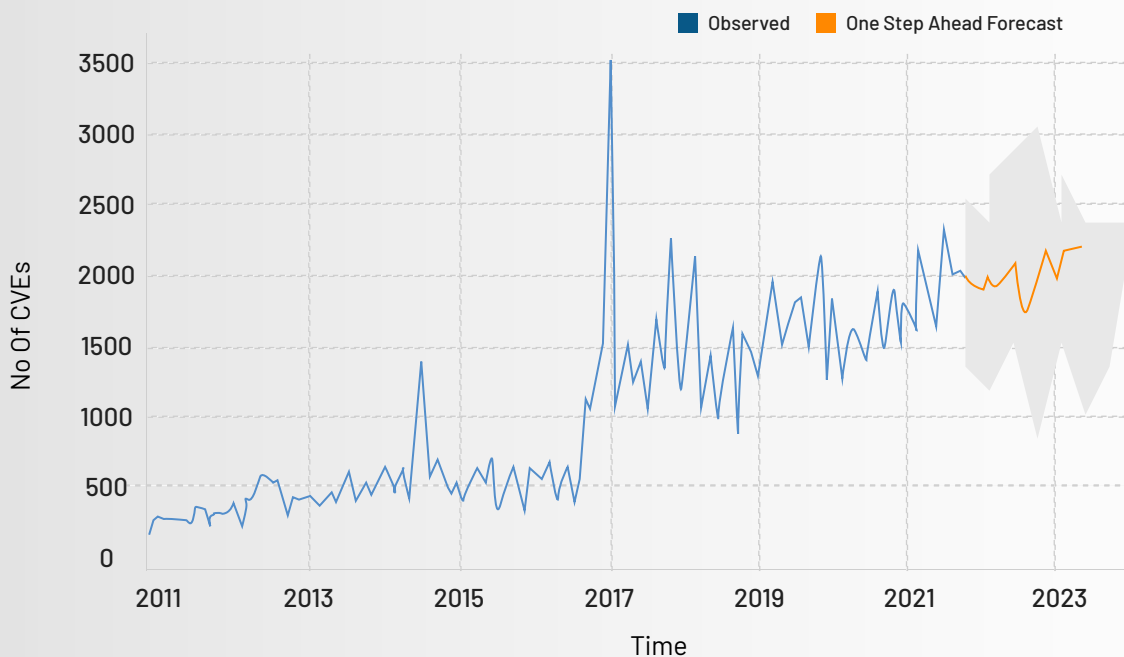


At SecPod, we compare all the discovered CVEs with our researched MVE (Malware Vulnerability Enumeration) data. With this, we identify the vulnerabilities which cause high-fidelity attacks. The number of vulnerabilities that can cause high-fidelity attacks has been the highest in the month of July. It 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.

# Keep Vulnerabilities in Check with SanerNow Advanced Vulnerability Management

The vulnerability landscape is massive and growing day-by-day. SanerNow Advanced Vulnerability Management provides you with a continuous and automated solution to manage different vulnerabilities including CVEs, misconfigurations, IT asset exposures, security control deviations, missing patches, and posture anomalies from a single centralized console. Leveraging the homegrown world's largest security intelligence library with more than 160,000 vulnerability checks, industry's fastest scans, and integrated remediation, SanerNow detects and remediates vulnerabilities at ease to keep cyberattacks at bay.

## 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)

Visit us at:

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