secpod

Q1 VULNERABILITY REPORT 2023

Q1 Vulnerability Report

It looks like 2023 has just started and we are already over the first quarter of the year. The first three months of 2023 (January to March) saw a total of 6963 vulnerabilities, 12 % more than the last three months of 2022. The first three months of 2023 also witnessed over 9 zero-days. It is evident that the numbers are rising every month and is only going to increase in the days to come. SecPod's security researchers are predicting over 31000 vulnerabilities this year. These vulnerabilities need continuous attention from the IT security teams to safeguard network from potential security hazards.

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. 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 improve the security posture of your organization.

What the Report consist of

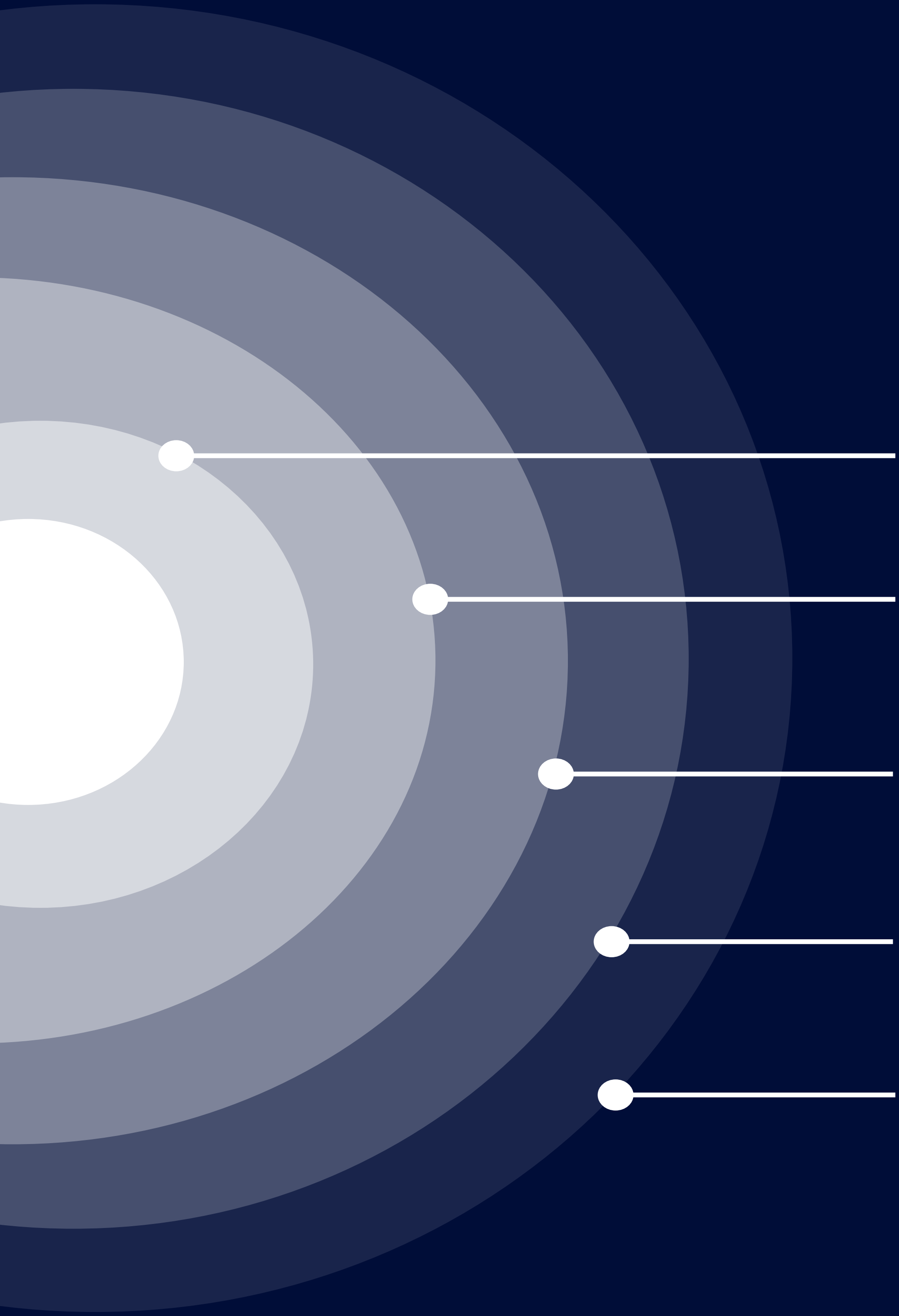
The report consist of the important details of the vulnerabilities that were discovered from January to March 2023. Note that the vulnerability details are researched and mentioned in the report based on the publish date. You will find detailed insights on the following:

- Key Findings from SecPod's Security Research Team
- SecPod's Security Intelligence Coverage from January to March 2023
- Total Number of Vulnerabilities
- Vulnerability Distribution based on CVSS v3 Algorithm, Exploitability Score, and Impact Score
- Top 10 Affected Vendors/Products
- Top 10 Affected Operating Systems
- Top 10 Affected Applications
- Top 10 Affected Hardware
- Top 10 Most Critical Vulnerabilities
- Analytics of Malware Vulnerability Enumeration [MVE]
- Vulnerability Prediction of the upcoming months using the ARIMA model

Key Findings from SecPod's Security Research Team

- 6963 is the number of vulnerabilities discovered between January and March 2023, 12 % more than the vulnerabilities discovered in last quarter of 2022.
- As per CVSS v3, 3937 vulnerabilities were reported with critical & high severity in the first quarter of 2023, 3.8 % more than the last quarter of 2022.
- 9 zero days were discovered in the first quarter of 2023.
- 51 of the total vulnerabilities discovered between January and March 2023 are widely exploited.
- 8 of the total vulnerabilities discovered in the first quarter of 2023 have public exploits available.
- 43 of the total vulnerabilities discovered in the first quarter of 2023 are Malware Exploiting Vulnerabilities, causing High-fidelity attacks
- 94 web browser vulnerabilities were discovered in the first quarter of 2023.

Vulnerability Trend– Q1, 2023



Total number of vulnerabilities: 6963

Vulnerabilities with critical & high severity as per CVSS v3: 3937

Vulnerabilities causing high-fidelity attacks: 43

Widely exploited Vulnerabilities: 51

Vulnerabilities with public exploit available: 8

SecPod's Security Intelligence Coverage from January to March 2023

Advanced Vulnerability Coverage

- Total No of CVEs Covered: 4186
- No of Local Checks: 4908 (No of security checks scanned by agent, other is network scanner)
- No of Remote Checks: 24
- Zero-day CVEs covered: 9
- CISA Vulnerabilities Coverage: 764/906
- Network Device Vulnerabilities: 17
- Total No of Misconfigurations covered: 183

CVE Coverage based on platforms

- Windows - 740
- Linux - 3316
- macOS – 429

Common Remediation Enumeration (CRE) Coverage

- Total No of Patches Covered: 311
- Total No of Third-party applications Patches Covered: 326
- Total No of Misconfigurations patches covered: 125
- Total No of OS Patches Covered: All latest Versions for the Supported OS

SecPod's Security Intelligence Coverage from January to March 2023 continued...

Compliance Benchmark Coverage Between January and March

- Debian 11
- Debian 11 NIST 800-53
- Debian 11 NIST 800-171
- Debian 11 HIPAA

*NOTE: General Compliance is the combination of numerous industry benchmarks

Number of CVEs Published from January to March 2023

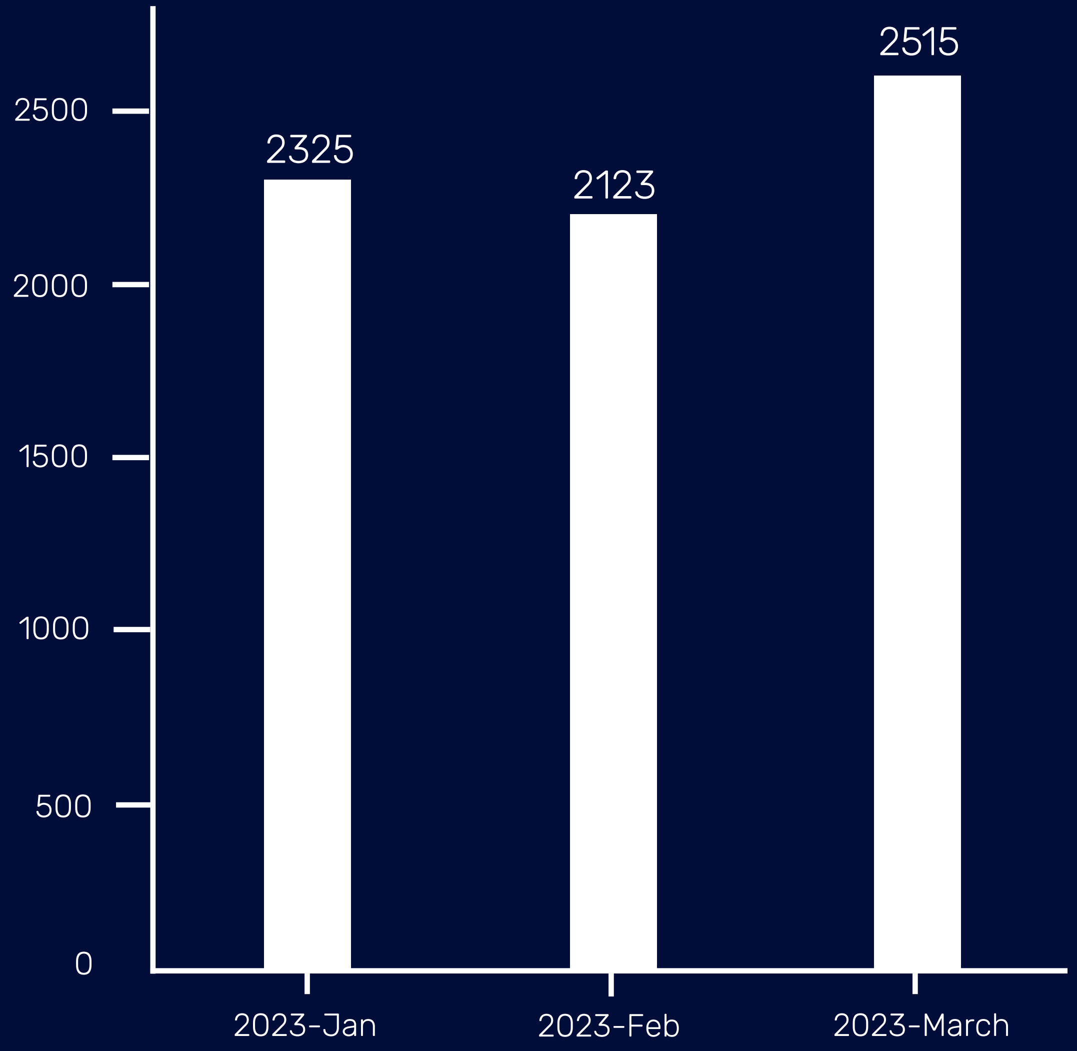


Figure 1: Shows the Number of vulnerabilities published from January to March 2023

The number of vulnerabilities published in the first quarter of 2023 is 6963, 12 % more than the 6226 vulnerabilities published in the last three months of 2022. This list includes a total of 9 zero-day vulnerabilities.

Vulnerability Severity Distribution as per CVSS v3 score

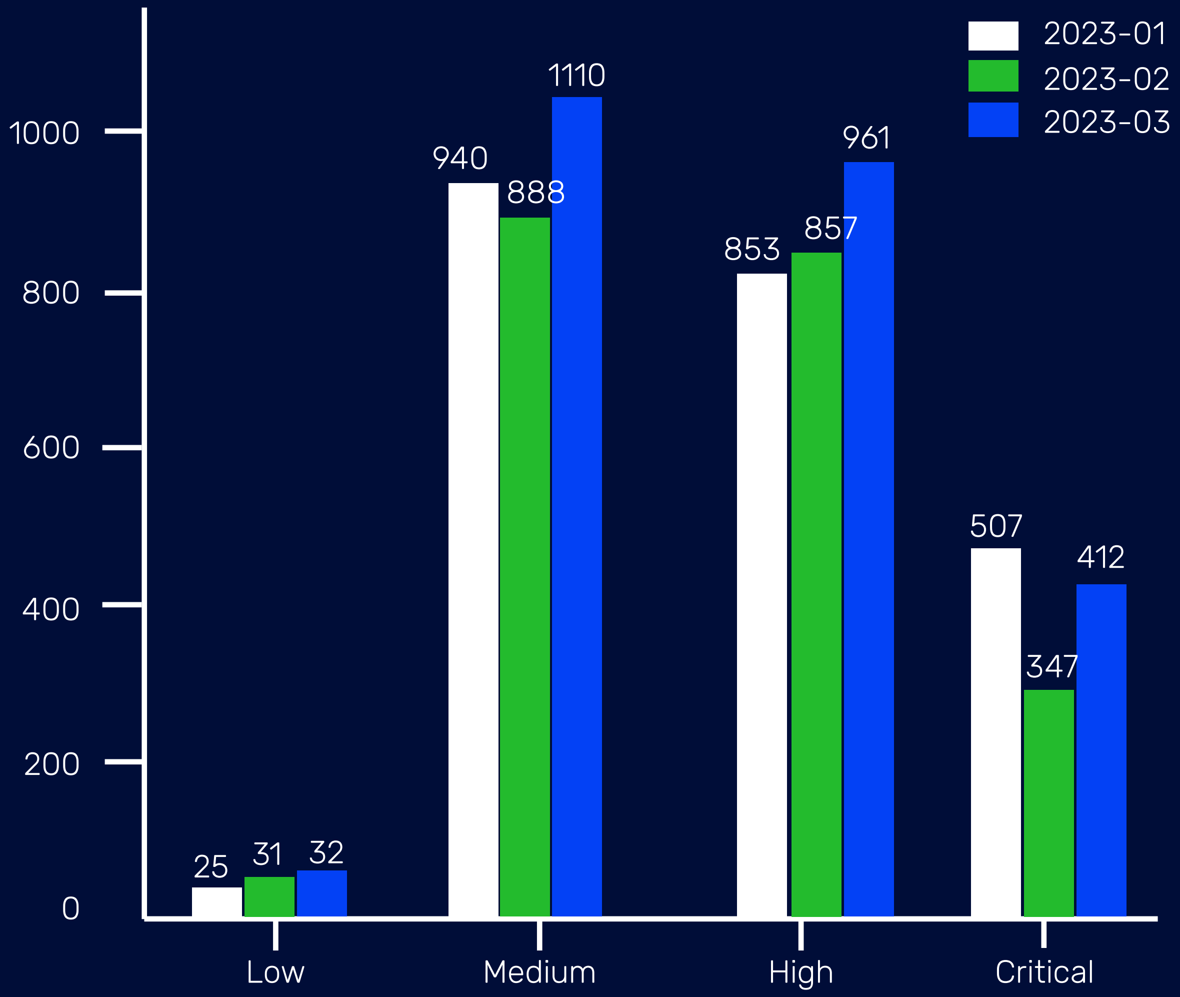


Figure 2: Depicts the vulnerability severity distribution based on CVSS v3

As per the CVSS v3 score, 1266 vulnerabilities are reported with critical severity, and 2671 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

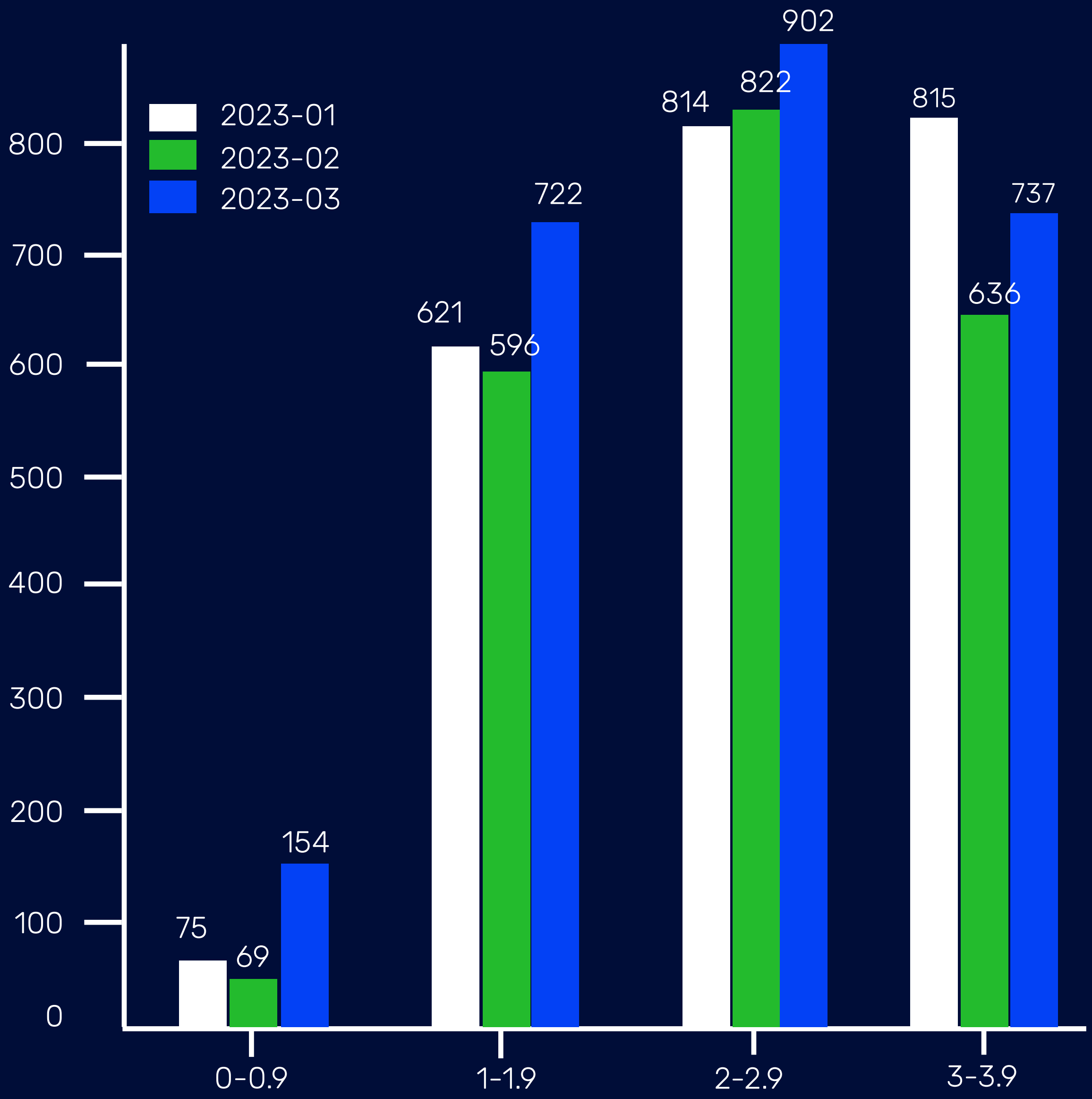


Figure 3: Depicts the distribution of vulnerabilities based on the exploitability score of CVSS v3

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

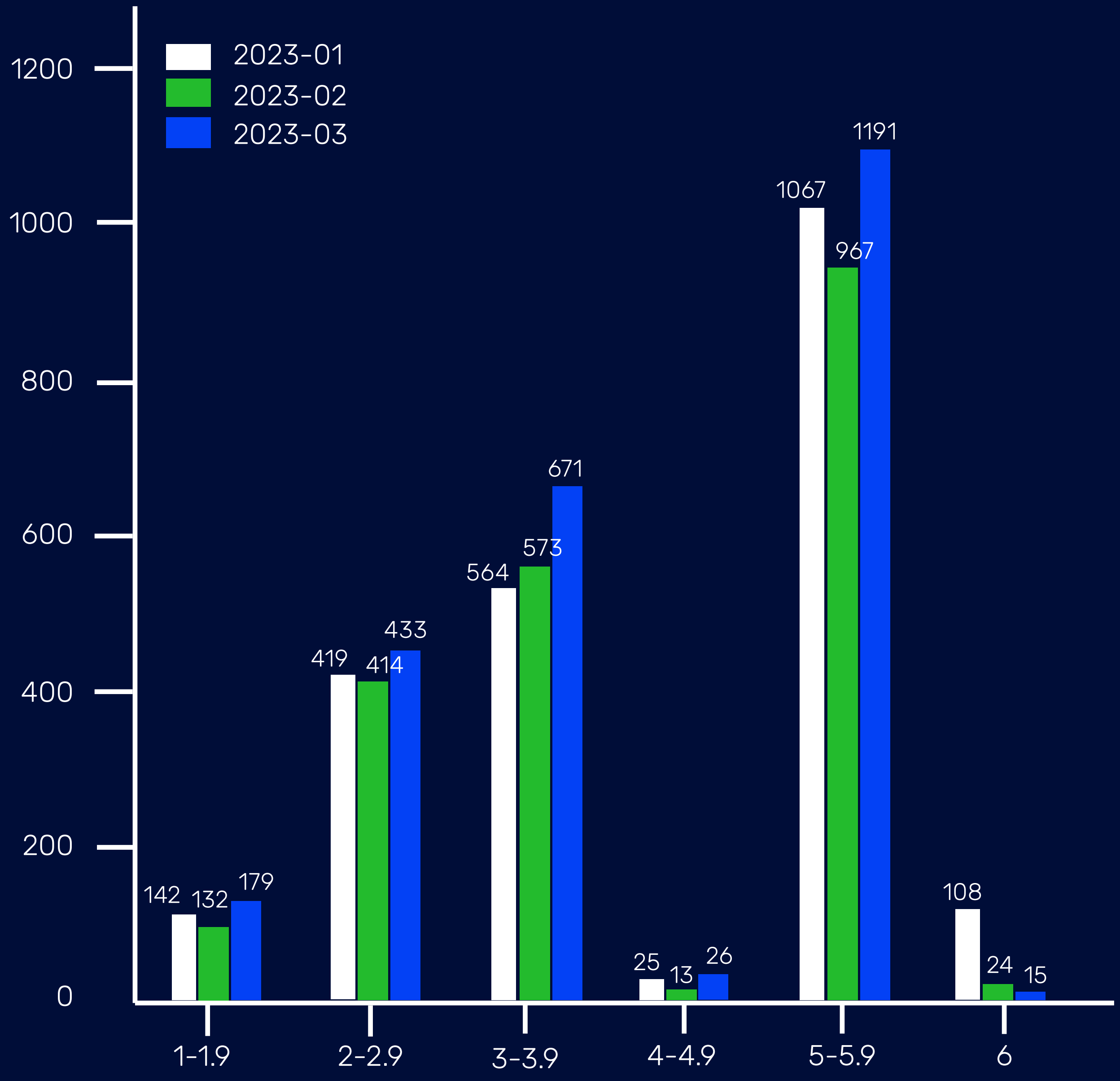


Figure 4: Depicts the distribution of vulnerabilities based on the impact score of CVSS v3

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

Top 10 Affected Vendors/Products

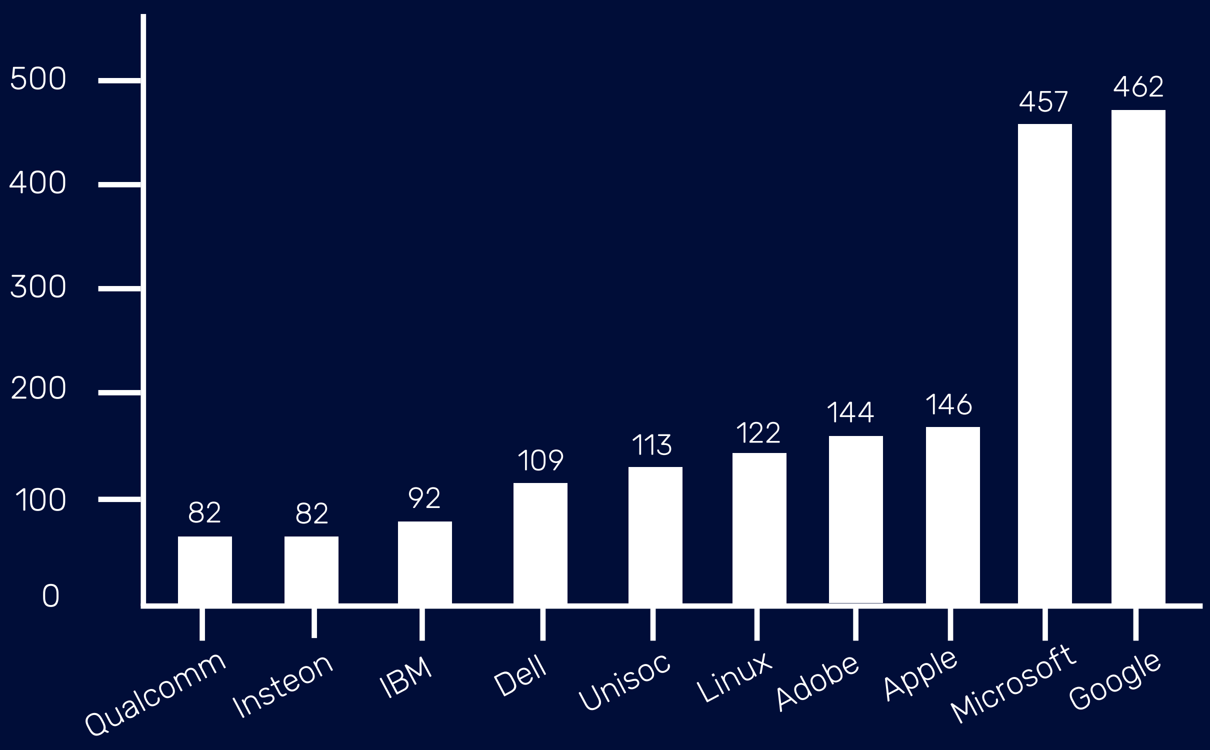


Figure 5: Shows the Top 10 vendors affected by CVEs

Microsoft and Google are the most affected Vendors in the first quarter of 2023. Respectively they have reported 457 and 462 vulnerabilities each.

Top 10 Affected Operating Systems

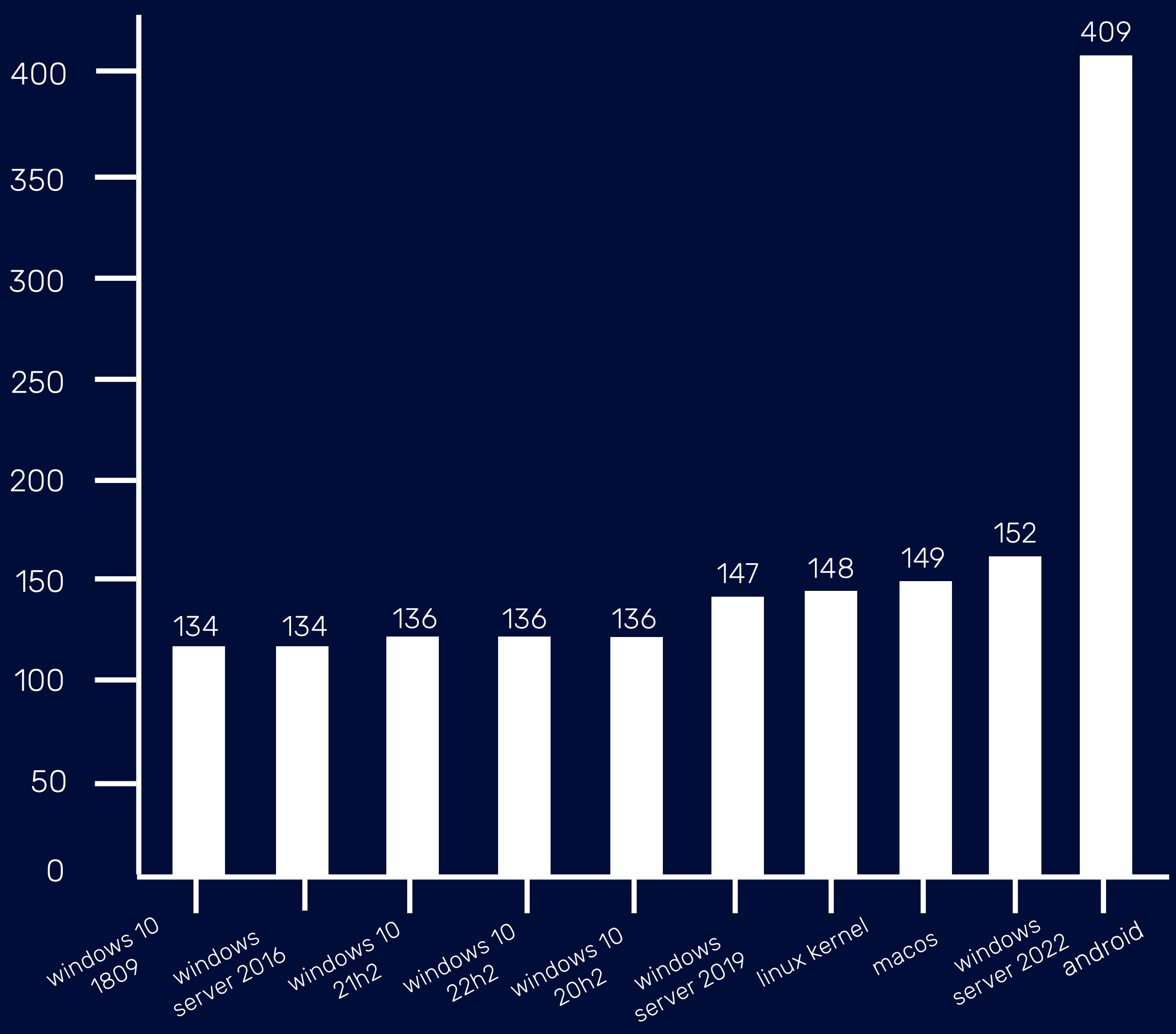


Figure 9: Shows the Top 10 Operating Systems Affected by CVEs

Android is the most affected operating system, with a total of 409 vulnerabilities. Windows operating system also report a fair share of vulnerabilities.

Top 10 Affected Hardware

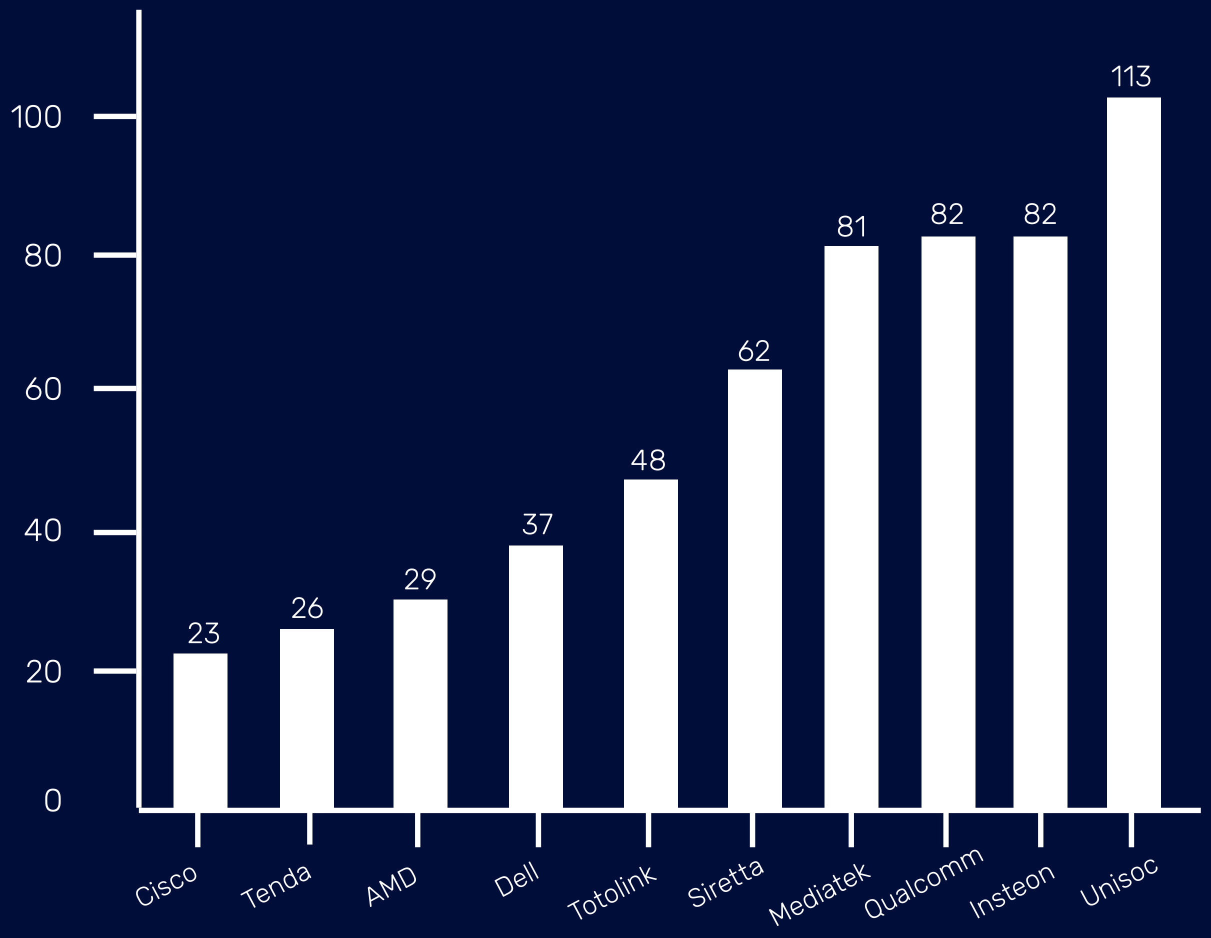


Figure 11: Shows the Top 10 Hardware Affected by CVEs

Unisoc is the most affected hardware in the first three months of 2023 and has reported over 113 vulnerabilities.

Top 10 Most Critical Vulnerabilities

This section provides the details of the Top 10 most critical vulnerabilities discovered between January and March 2023. 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 Score	Impact
01	CVE-2022-23521 & CVE-2022-41903	git	9.8	Integer Overflow
02	CVE-2023-22501	Jira Service Management Server Jira Service Management Data Center	9.4	Improper Authentication
03	CVE-2022-44877	Centos Web Panel	9.8	Remote Code Execution
04	CVE-2021-42756	FortiWeb's proxy daemon	9.3	Remote Code Execution
05	CVE-2022-47966	Multiple ManageEngine Products	9.8	Remote Code Execution
06	CVE-2023-23397	Microsoft Outlook	9.8	Authentication Bypass
07	CVE-2023-23529	Apple Mac OS and Safari	8.8	Remote Code Execution
08	CVE-2023-21823	Microsoft Windows	7.8	Remote Code Execution
09	CVE-2023-23376	Microsoft Windows	7.9	Privilege Escalation
10	CVE-2023-21768	Microsoft Windows	7.8	Privilege Escalation

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

Zero Days Discovered between January and March 2023

This section consists of the details of the CVEs discovered between January and March 2022. The following 9 zero days were discovered in this quarter.

S. No	CVE ID	Affected Products	CVSS Score	Impact
01	CVE-2023-21674	Microsoft Windows	8.8	Privilege Escalation
02	CVE-2023-23529	Apple macOS and Safari	8.8	Remote Code Execution
03	CVE-2023-21823	Microsoft Windows	7.8	Remote Code Execution
04	CVE-2023-23376	Microsoft Windows	7.8	Privilege Escalation
05	CVE-2023-20963	Google Android	7.8	Privilege Escalation
06	CVE-2023-23397	Microsoft Outlook	9.8	Privilege Escalation
07	CVE-2023-21768	Microsoft Windows	7.8	Privilege Escalation
08	CVE-2023-0266	Google Android	7.8	Privilege Escalation
09	CVE-2023-26083	ARM Android	5.5	Privilege Escalation

Patches are available to fix all the zero-day vulnerabilities mentioned in the table

Analysis of High-Fidelity Attacks

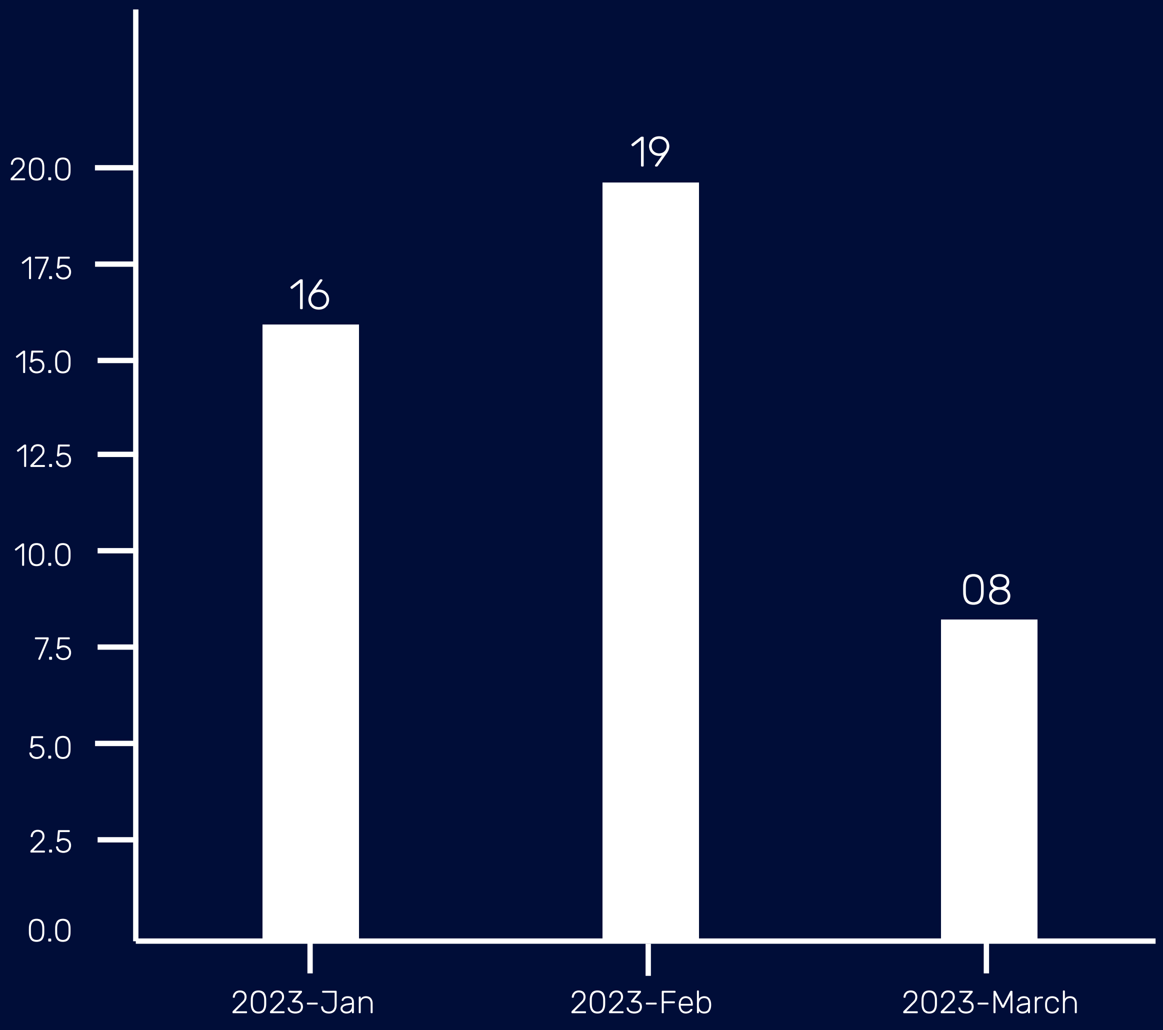
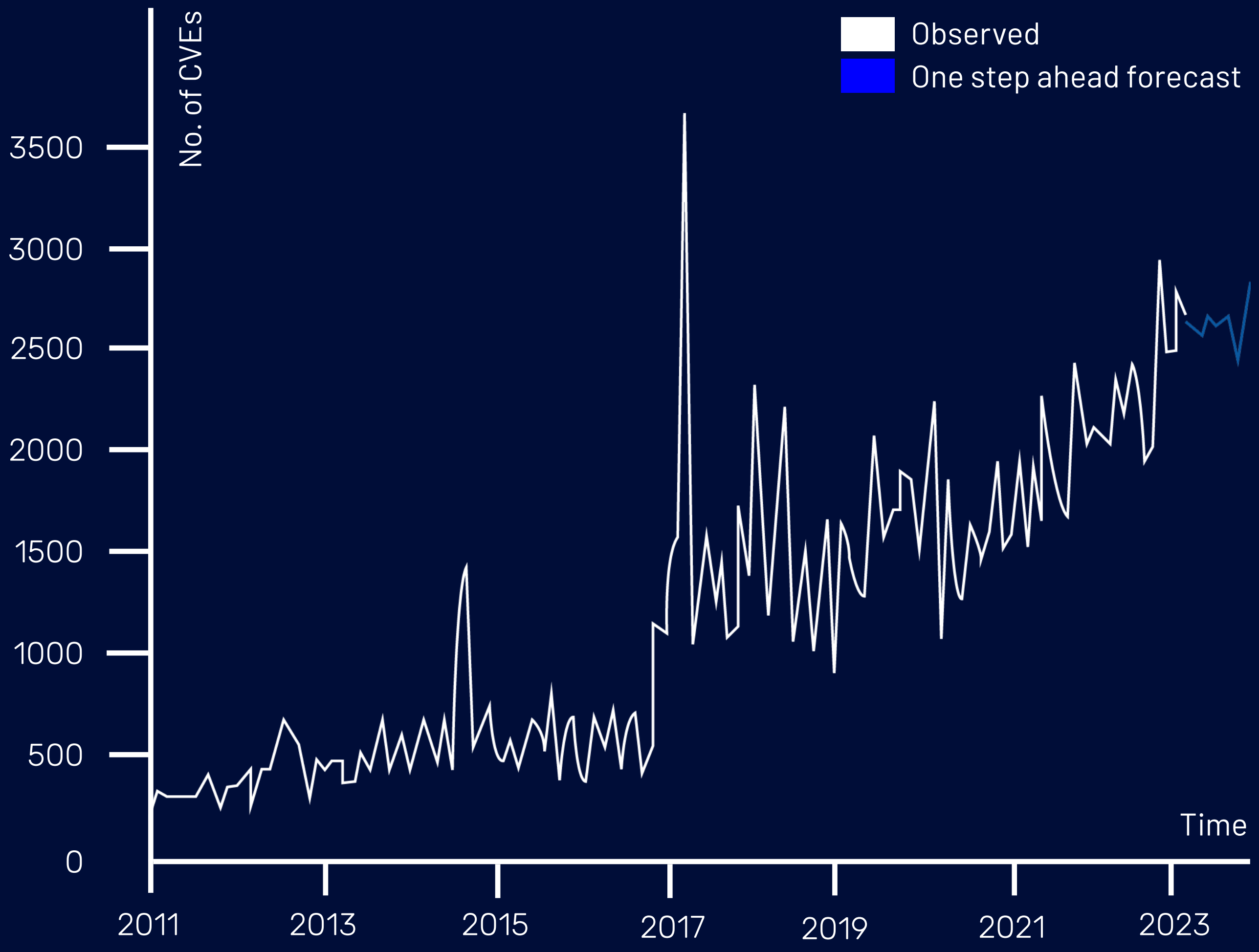


Figure 12: Depicts the monthly number of vulnerabilities that causes high-fidelity attacks

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 february. It is highly recommended that these vulnerabilities must be detected and remediated quickly to safeguard your network against cyberattacks.

Vulnerability Prediction 2023



On observing the vulnerability trend over the years, from SecPod, we predict over 31000 vulnerabilities in 2023. This prediction is made based on the ARIMA (Autoregressive Integrated Moving Average) model.

Top Anomalies Lurking in the organization's IT surface

Posture anomalies are the most obvious security risks that are hidden in the IT network and might lead to potential attacks. These anomalies need to be discovered and eliminated quickly to normalize IT infrastructure and prevent numerous cyberattacks. Based on our analysis, here are the top anomalies present in the organization's attack surface that needs to be identified and acted upon immediately.

- Unique services running only in select systems
- Unique software applications installed in few devices
- Installation of Unsigned Applications
- Unusual tasks scheduled in Task Scheduler
- Applications making outbound connections to unusual ports

Discover and Eliminate Vulnerabilities with SanerNow Advanced Vulnerability Management

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 170,000 vulnerability checks, industry's fastest scans, and integrated remediation, SanerNow detects and remediates vulnerabilities at ease to keep cyberattacks at bay.

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.

info@secpod.com

secpod