secpod

Autumn

VULNERABILITY REPORT 2023

www.secpod.com

Autumn Vulnerability Report 2023

We are almost nearing the end of 2023 and have witnessed 21780 vulnerabilities till September 2023. SecPod's security research reveals that the third quarter of 2023 experienced a total of 6944 vulnerabilities, including 17 zero-day vulnerabilities. Zero-day vulnerabilities are clearly on the rise, and tools that can instantly remediate are in demand. These vulnerabilities, when left unattended, will open gateways for cyber attackers to exploit your organization's network. According to SecPod's security intelligence, the predicted vulnerabilities at the end of 2023 is 31,000; staying informed about the vulnerability trends is crucial to defend against cyberattacks effectively.

At SecPod, we are dedicated to keeping you informed about the latest vulnerability information through our quarterly vulnerability reports. As part of this report, we have compiled insights into the vulnerabilities observed between July and September 2023. This report highlights the latest vulnerability trends and outlines the top critical vulnerabilities discovered during the third quarter of the year. We strongly recommend that you promptly address these high-risk vulnerabilities within your network to maintain a proactive stance against potential attackers and mitigate any security incidents. Let us now delve into the details of the vulnerability trends from July to September 2023.

> *As with every quarter, we see an increasing trend in new vulnerabilities being discovered and weaponized to launch attacks. Vulnerabilities remain the attacker's most sought-after exploitable attack vector. At SecPod, we are continually advancing our approach with technology and tools to help our Customers build an effective vulnerability management program. We have introduced a new tool, SanerNow RP, to prioritize vulnerability. Also, a thought-provoking framework called CVEM is introduced that our platform implements.*

Chandrashekhar Basavanna, CEO, SecPod

What does the Report consist of?

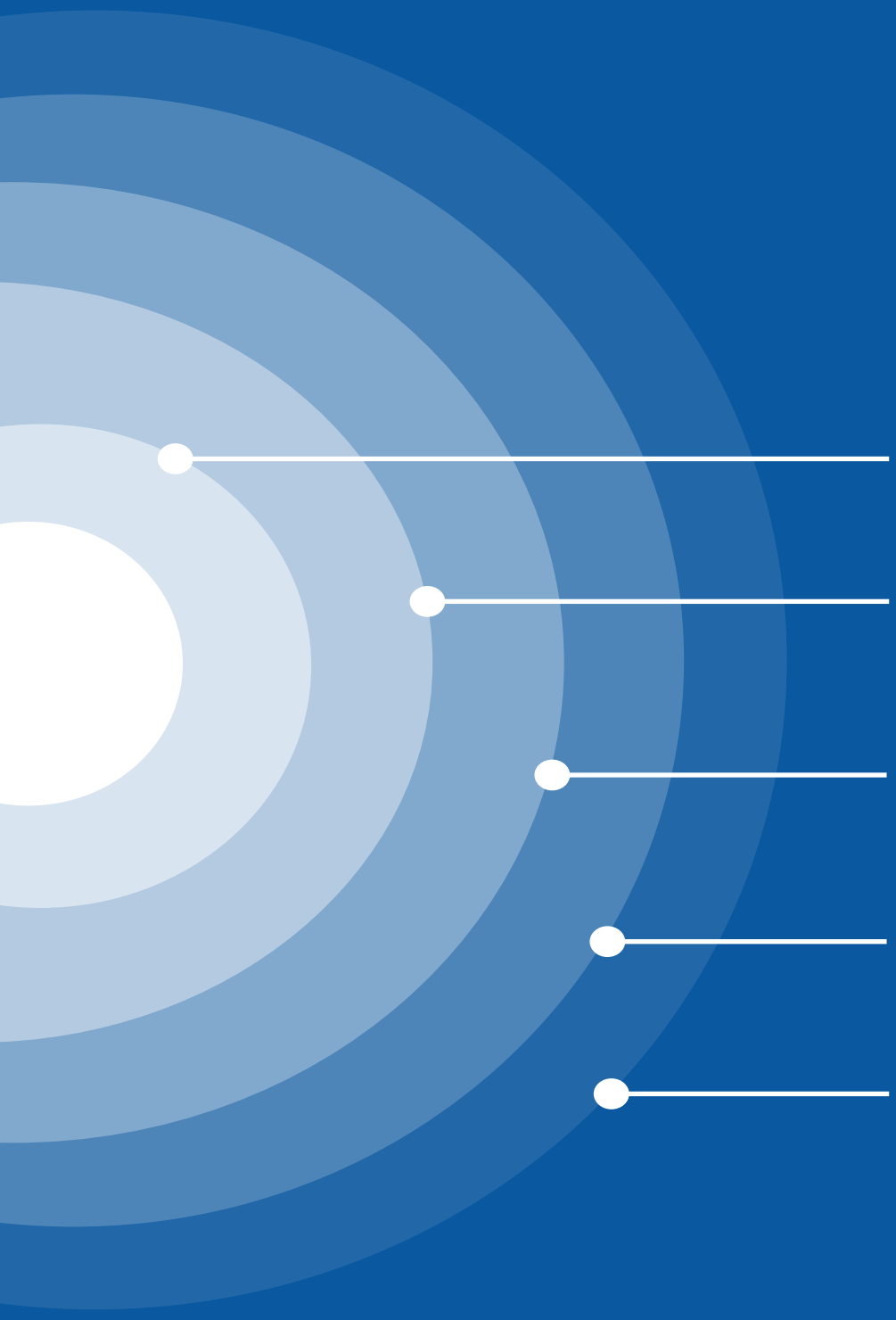
The reports consist of the important details of the vulnerabilities that were discovered from July to September 2023. The vulnerability details are researched and mentioned in the report based on the publish date.
You will find detailed insights on the following:

- Key Findings from SecPod's Security Research Team
- SecPod's Security Intelligence Coverage from July to September 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

- 6944 is the total number of vulnerabilities discovered between July and September 2023.
- As per CVSS v3, 3661 vulnerabilities were reported with critical & high severity in the third quarter of 2023.
- 27 of the total vulnerabilities discovered in the third quarter of 2023 have public exploits available.
- 17 zero days were discovered in the third quarter of 2023.
- 37 of the total vulnerabilities discovered between July and September 2023 are widely exploited.
- 33 of the total vulnerabilities discovered in the third quarter of 2023 got the potential of High-fidelity attacks and are Malware Exploiting Vulnerabilities
- 197 web browser vulnerabilities were discovered in the third quarter of 2023.

Vulnerability Trend July-September 2023



Total number of vulnerabilities: 6944

Vulnerabilities with critical & high severity as per CVSS v3: 3661

Vulnerabilities with public exploit available: 27

Widely exploited Vulnerabilities: 37

Vulnerabilities causing high-fidelity attacks: 33

secpod

SecPod's Security Intelligence Coverage from July to September 2023

Advanced Vulnerability Coverage

- Total No of CVEs Covered: 4180
- No of Local Checks: 6088 (No of security checks scanned by agent, other is network scanner)
- No. of Remote Checks: 157
- CISA Vulnerabilities Coverage: 870
- Zero-day CVEs covered: 17

CVE Coverage based on platforms

- Windows - 1049
- Linux - 2522
- macOS – 392

- Common Remediation Enumeration Coverage (CRE): 578
- Network Device Vulnerabilities: 550
- Total No of Misconfigurations Covered: 183
- Total No of Patches Covered: 479
- Total No of Third-party applications Patches Covered: 238
- Total No of Misconfigurations patches covered: 241

Compliance Benchmark Coverage between July and September

- Windows Server 2019 STIG Coverage
- Ubuntu 23.04 Benchmarks revised
- Windows Server 2022 STIG Coverage

secpod

Total Number of CVEs Covered

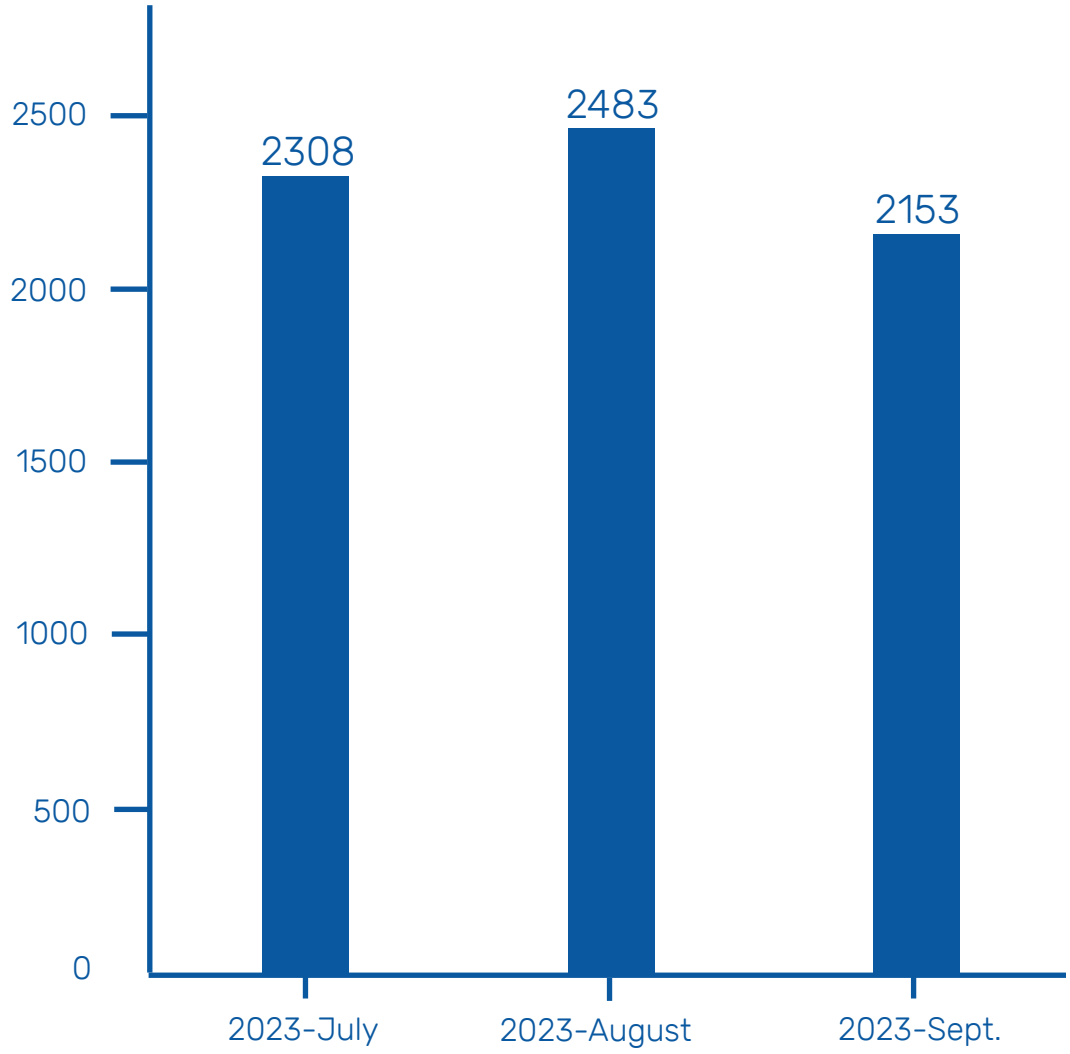


Figure 1: Shows the number of vulnerabilities published from July to September 2023

The number of vulnerabilities published in the third quarter of 2023 is 6944. This list includes a total of 17 zero-day vulnerabilities.

Vulnerability Severity Distribution based on CVSS v3

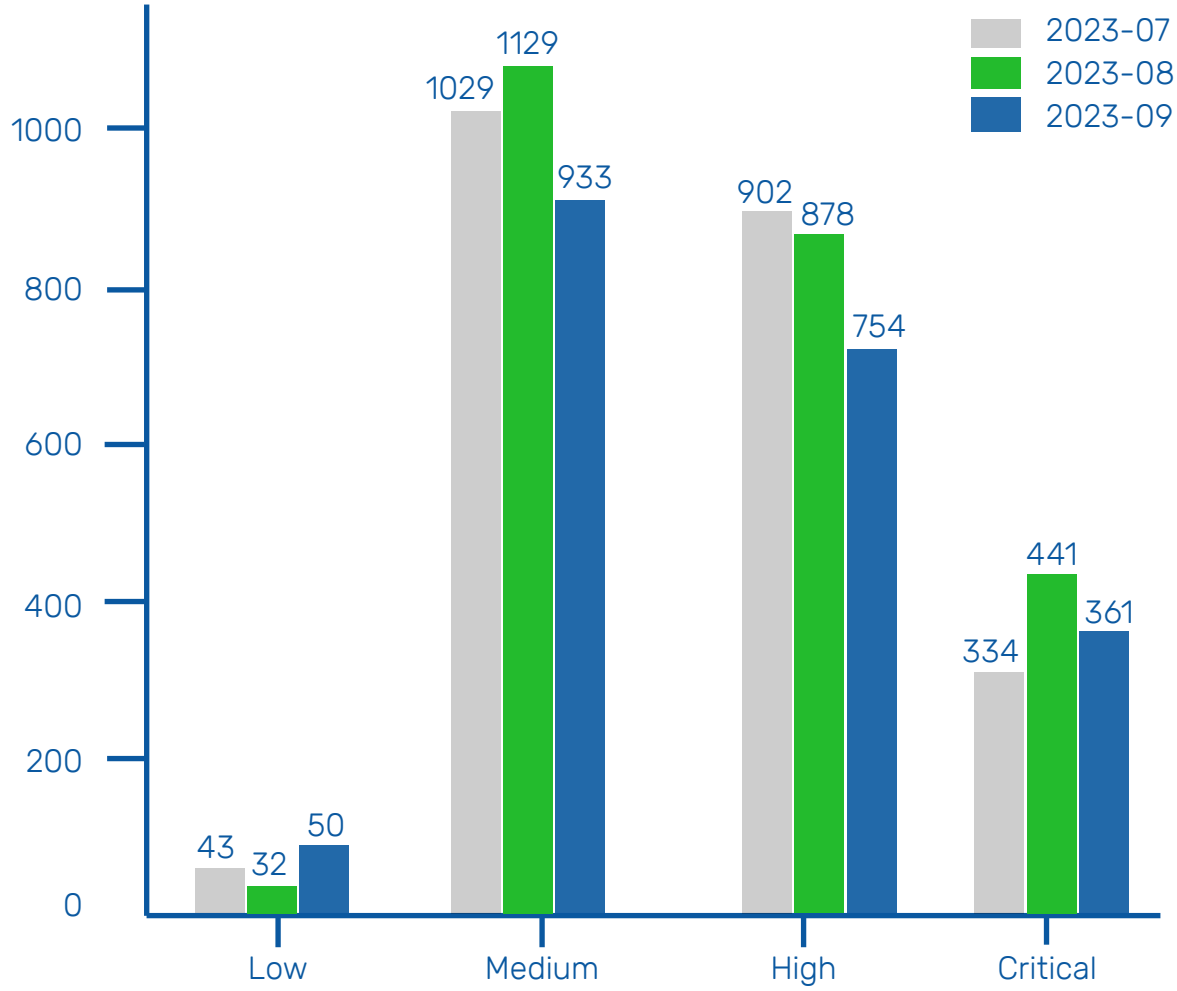


Figure 2: Depicts the vulnerability severity distribution based on CVSS v3 base score

As per CVSS v3 score, 125 vulnerabilities were reported with low severity, 3091 vulnerabilities were reported with medium severity, 2525 vulnerabilities were reported with high severity, and 1136 vulnerabilities were reported critical.

Vulnerability Severity Distribution based on CVSS v3 Exploitability Score

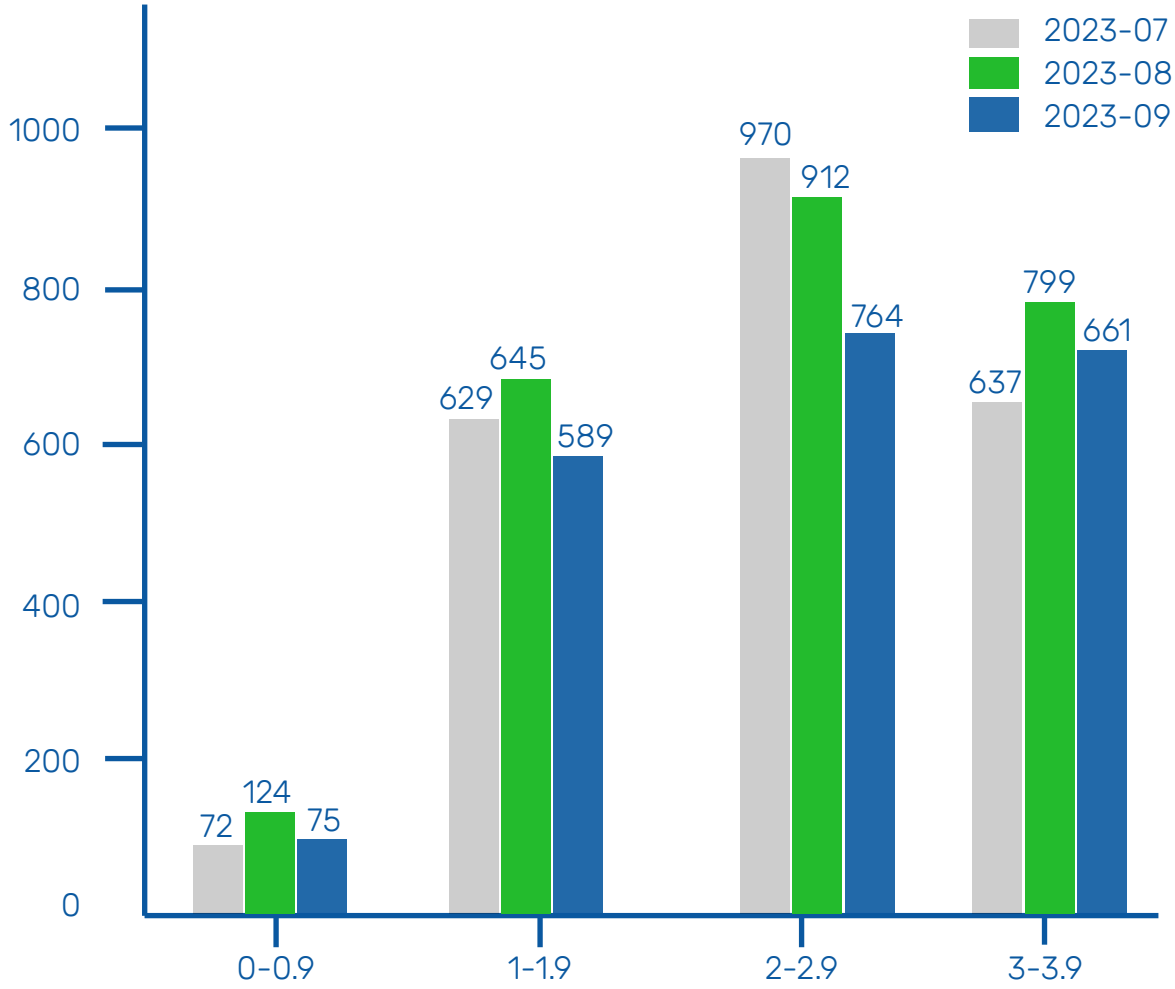


Figure 3: Depicts the distribution of vulnerabilities based on the exploitability score of CVSS v3

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

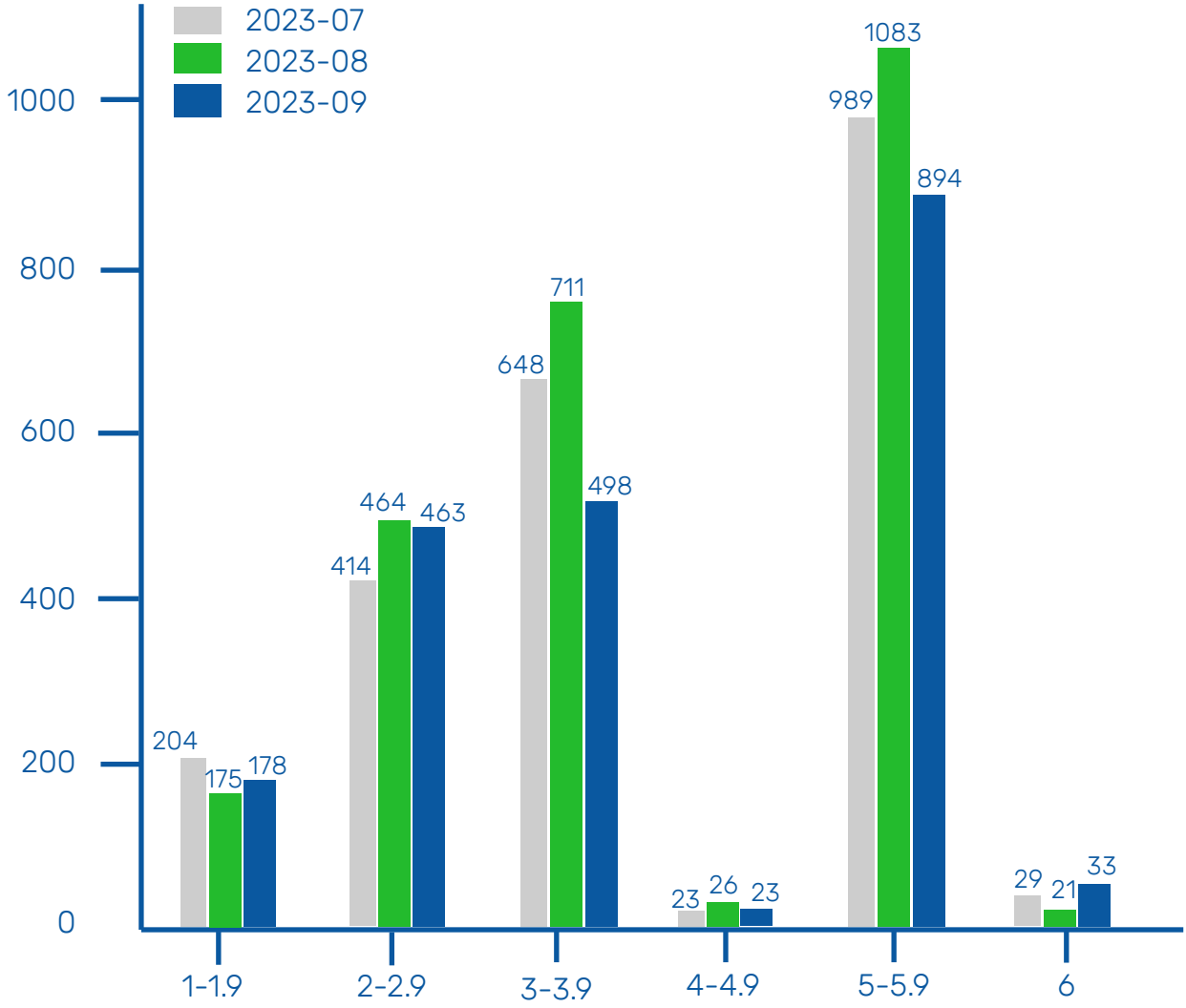


Figure 4: Depicts the distribution of vulnerabilities based on the impact score of CVSS v3

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

Top 10 Affected Vendors/Products

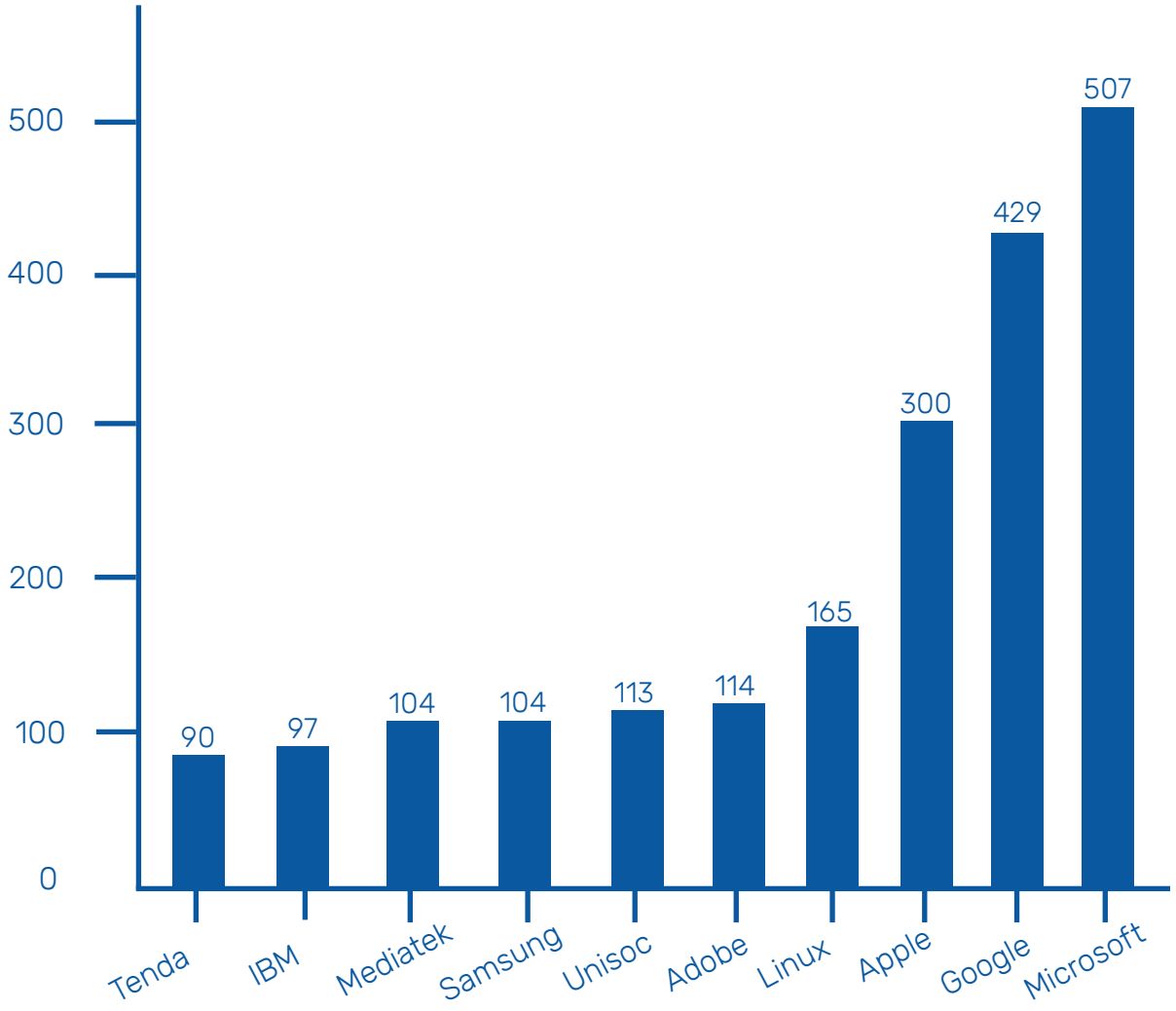


Figure 5: Shows the Top 10 vendors affected by CVEs

Microsoft and Google are the most affected Vendors in the third quarter of 2023. Respectively, they have reported 507 and 429 vulnerabilities each.

Top 10 Affected Operating Systems

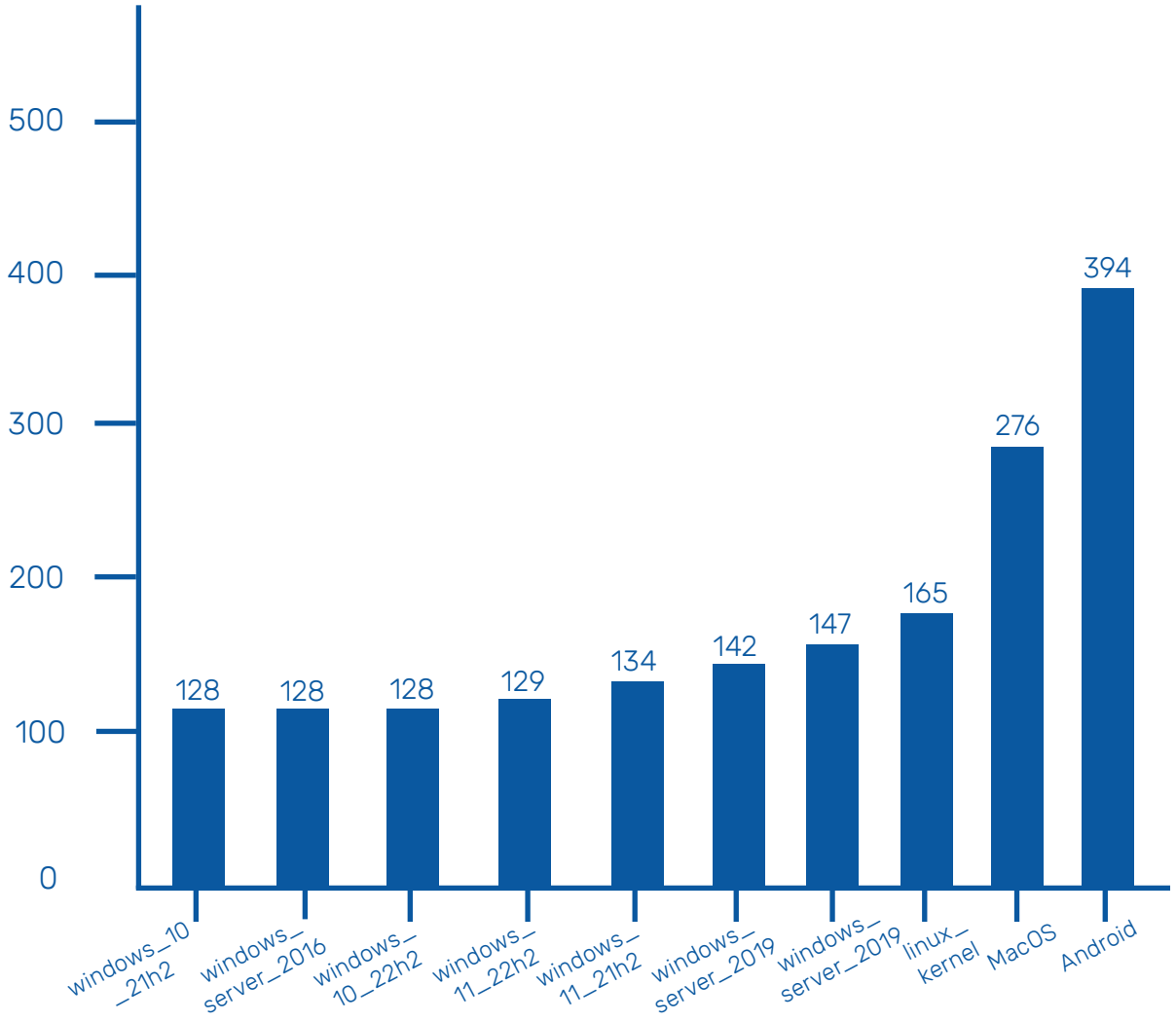


Figure 6: Shows the Top 10 Operating Systems Affected by CVEs

Android is the most affected operating system, with a total of 394 vulnerabilities. MacOS and Linux operating systems also report a fair share of vulnerabilities.

Top 10 Affected Hardware

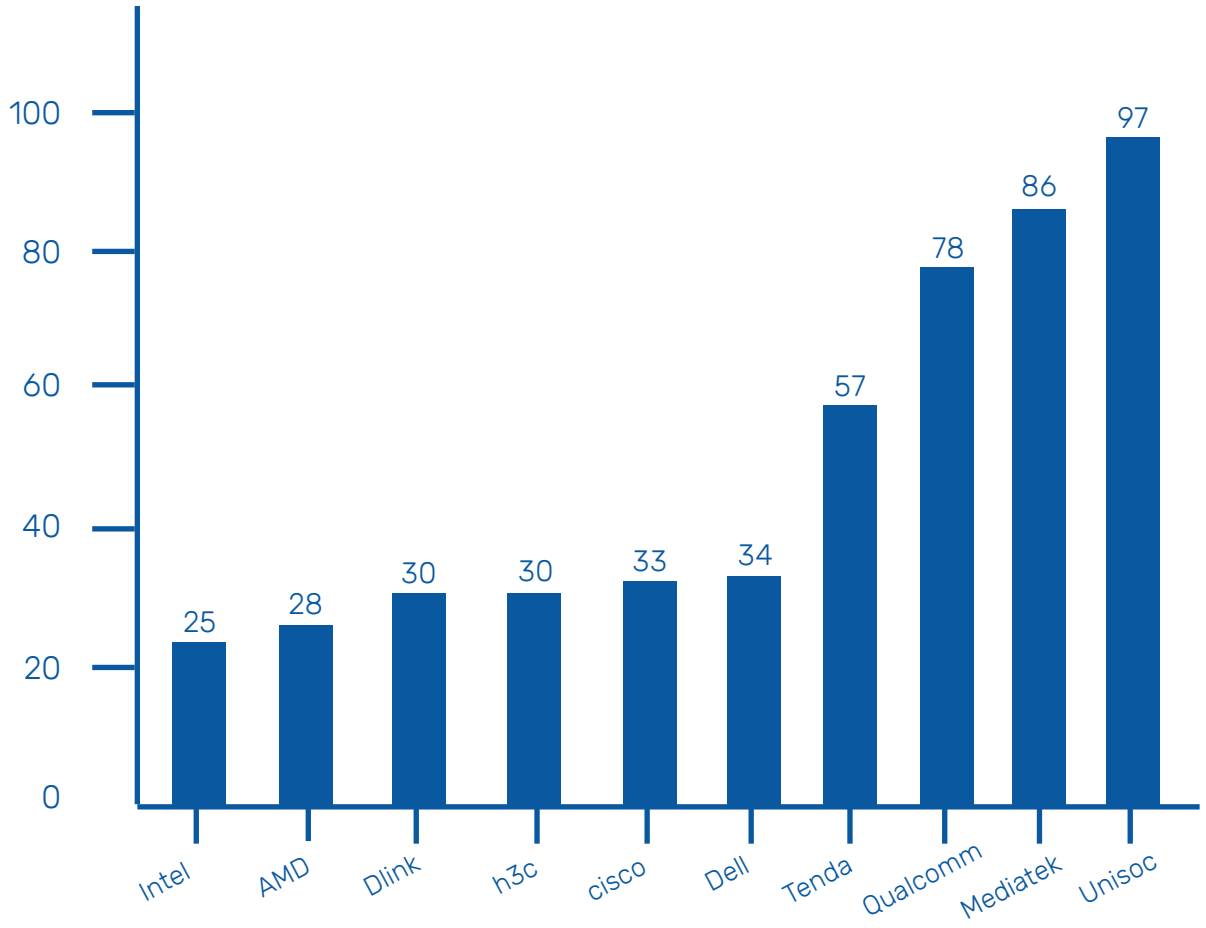


Figure 7: Shows the Top 10 Hardware Affected by CVEs

Unisoc has reported the highest number of vulnerabilities in the third quarter of 2023. It has reported 113 vulnerabilities in this quarter.

Top 10 Affected Applications

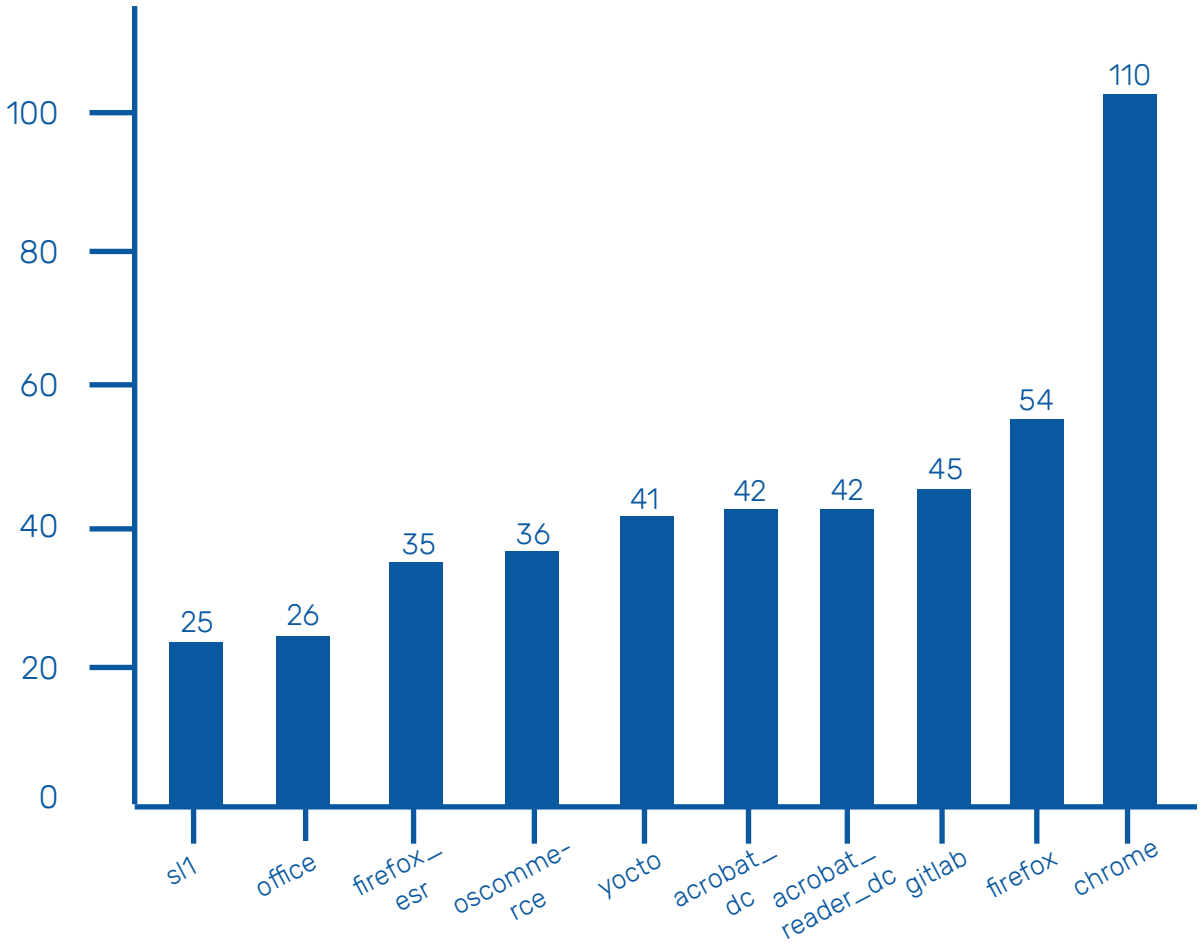


Figure 8: Shows the Top 10 Affected Applications by CVEs

Chrome has been the top-affected application in the third quarter of 2023, with 110 vulnerabilities.

Top 10 Most Critical Vulnerabilities

This section provides the details of the Top 10 most critical vulnerabilities discovered between July and September 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-2023-38203	Adobe ColdFusion	9.8	Arbitrary Code Execution
02	CVE-2023-3519	NetScaler ADC and NetScaler Gateway	9.8	Arbitrary Code Execution
03	CVE-2023-35311	Microsoft Outlook	8.8	Privilege Escalation
04	CVE-2023-38180	.Net Framework and Visual Studio7.5	7.5	Denial of Service
05	CVE-2023-39143	PaperCut NG and PaperCut MF	9.8	Arbitrary Code Execution
06	CVE-2023-34124	SonicWall GMS and Analytics Web Services	9.8	Authentication Bypass

Top 10 Most Critical Vulnerabilities contd.

S. No	CVE ID	Affected Products	CVSS Score	Impact
07	CVE-2023-40044	WS_FTP Server	10	Arbitrary Code Execution
08	CVE-2023-26369	Adobe Reader and Acrobat	7.8	Arbitrary Code Execution
09	CVE-2023-5217	Google Chrome	8.8	Arbitrary Code Execution
10	CVE-2023-36802	Microsoft Windows	7.8	Privilege Escalation

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

Zero-Day Vulnerabilities between July to September 2023

This section consists of the details of the CVEs discovered between July and September 2023. The following 17 zero days were discovered in this quarter.

S. No	CVE ID	Affected Products	Impact	CVSS Score
01	CVE-2023-32046	Microsoft Windows	Privilege Escalation	7.8
02	CVE-2023-36874	Microsoft Windows	Privilege Escalation	7.8
03	CVE-2023-36884	Microsoft Windows	Arbitrary Code Execution	8.8
04	CVE-2023-37580	Zimbra Classic Web Client	Arbitrary Code Execution	6.1
05	CVE-2023-38606	Apple iOS/macOS	Privilege Escalation	5.5
06	CVE-2023-32409	Apple macOS	Privilege Escalation	8.6
07	CVE-2023-38831	RARLabs WinRAR	Arbitrary Code Execution	7.8

Zero-Day Vulnerabilities between July to September 2023 contd.

S. No	CVE ID	Affected Products	Impact	CVSS Score
08	CVE-2023-4762	Google Chrome	Arbitrary Code Execution	8.8
09	CVE-2023-41064	Apple iOS/macOS	Arbitrary Code Execution	7.8
10	CVE-2023-4863	Google Chrome	Out-of-bounds Write	8.8
11	CVE-2023-26369	Adobe Reader	Arbitrary Code Execution	7.8
12	CVE-2023-36802	Microsoft Windows	Privilege Escalation	7.8
13	CVE-2023-36761	Microsoft Word	Information Disclosure	5.3
14	CVE-2023-41992	Apple iOS/macOS	Privilege Escalation	7.8
15	CVE-2023-41991	Apple iOS/macOS	Security Bypass	5.5
16	CVE-2023-41993	Apple iOS/macOS	Arbitrary Code Execution	9.8
17	CVE-2023-5217	Google Chrome	Arbitrary Code Execution	N/A

Analysis of High-Fidelity Attacks

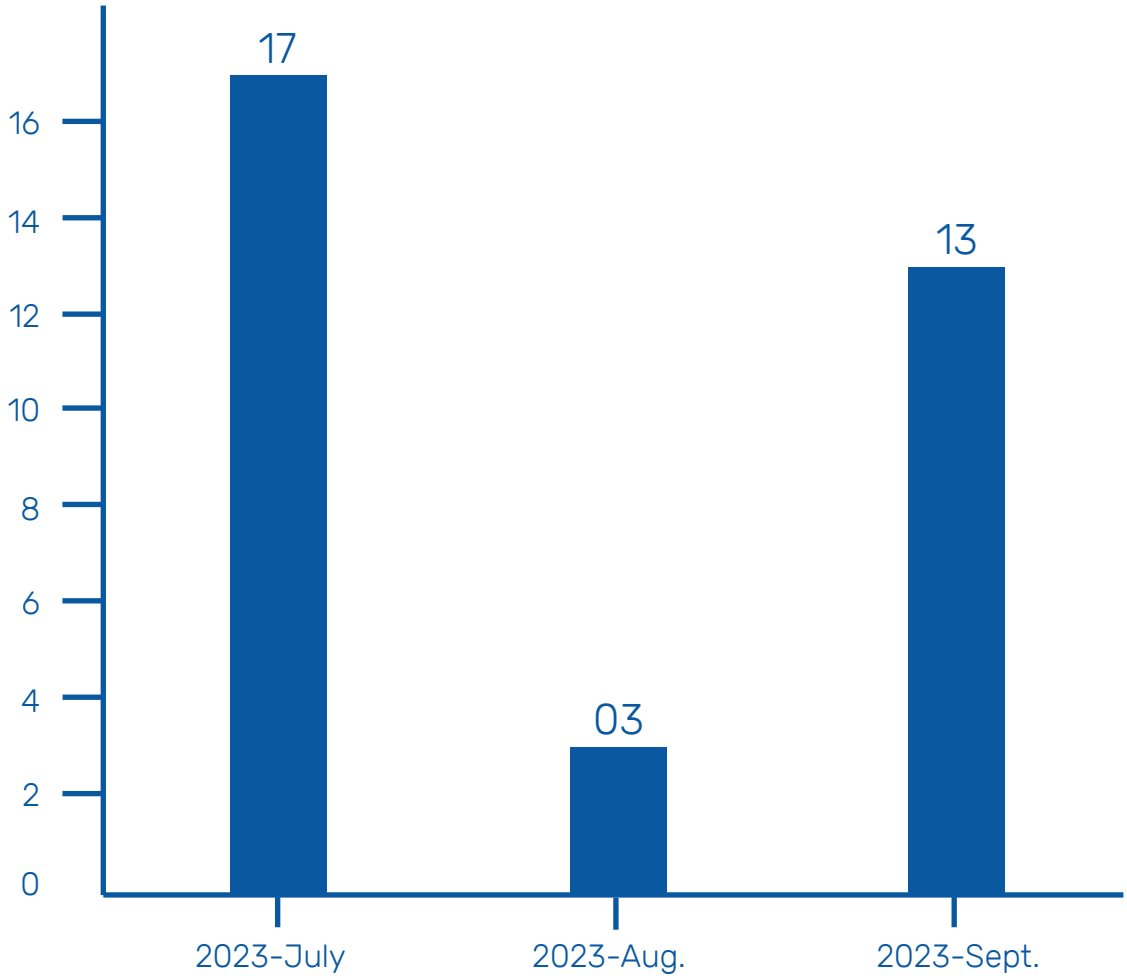


Figure 9: Depicts the monthly number of vulnerabilities that cause high fidelity attacks

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 is equally distributed in the month of July and September. It is highly recommended that these vulnerabilities must be detected and remediated quickly to safeguard your network against cyberattacks.

Analysis of Widely Exploited Vulnerabilities

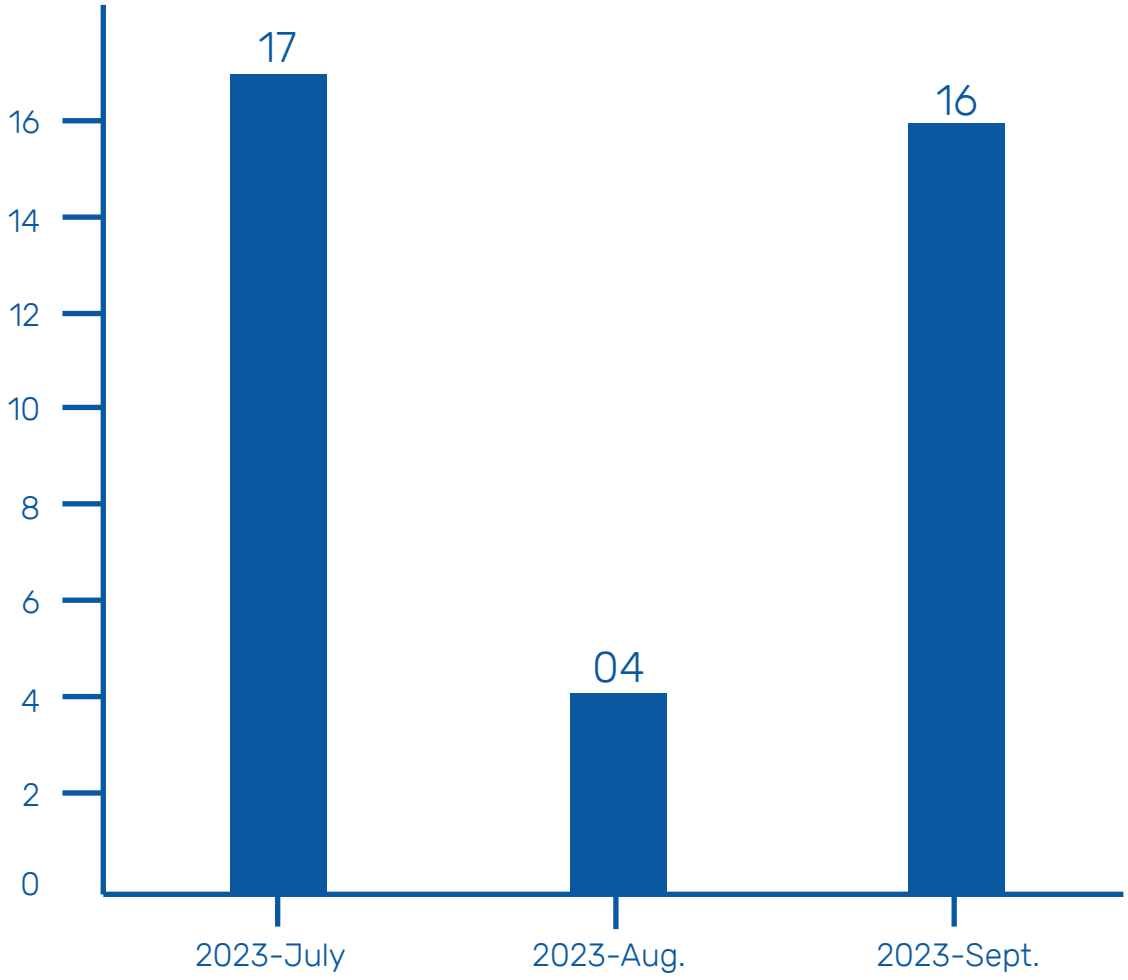


Figure 10: Depicts the monthly number of vulnerabilities that were widely exploited

Month of July experienced the most number of widely exploited vulnerabilities.

Vulnerability Prediction 2023

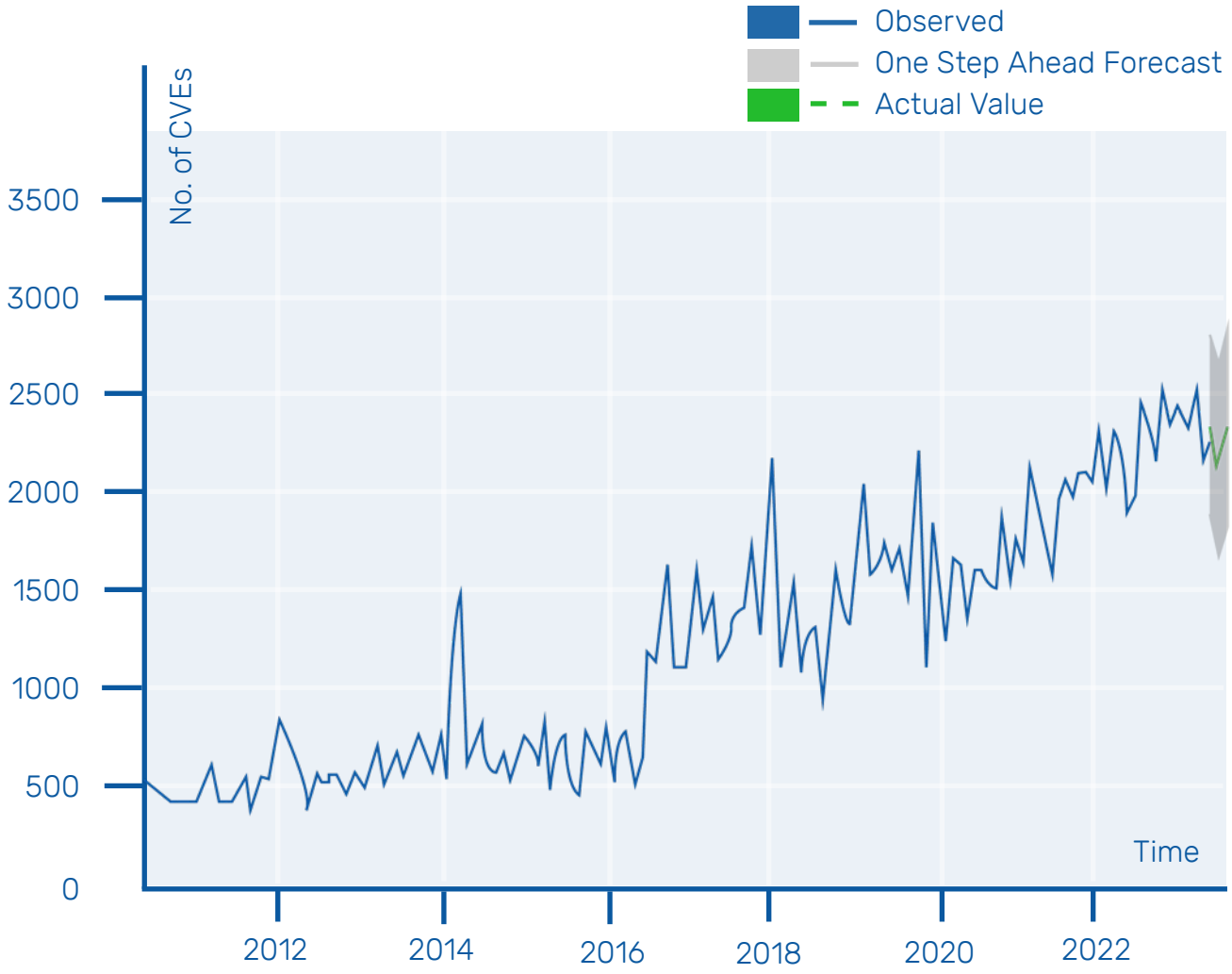


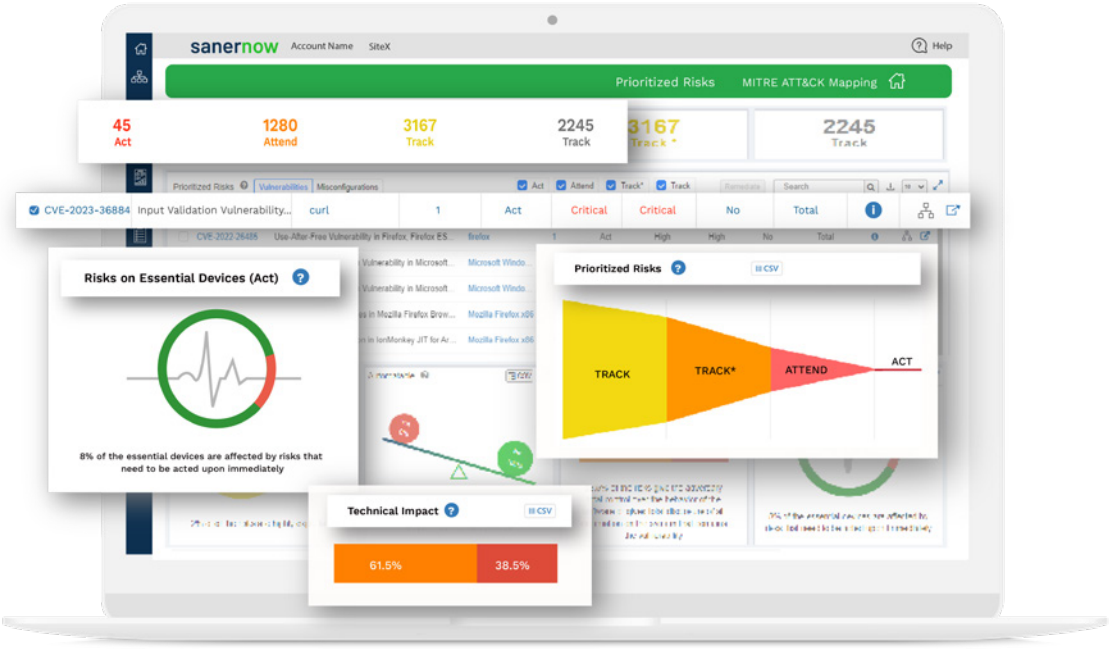
Figure 11: Forecasting Number of Vulnerabilities monthwise

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.

Simplify the Zillion to Zero Risk Journey with SanerNow Risk Prioritization

SanerNow Risk Prioritization (RP) is the world's first Stakeholder-Specific Vulnerability Categorization (SSVC) framework-based prioritization tool. It prioritizes vulnerabilities based on Business Context, and vulnerability characteristics such as Exploitability, Automatable, Technical Impact and Mission Prevalence parameters.

SanerNow RP, powered by in-house vulnerability and threat intelligence, implements an enhanced Exploit Prediction Scoring System (EPSS) and SecPod's unique risk categorization algorithm & proprietary mitigation evaluation techniques in the attack kill chain. SanerNow Risk Prioritization consumes raw vulnerability data from the natively integrated vulnerability scanners and business and environment context to prioritize vulnerabilities into Act, Attend, Track* & Track. It provides real-time insights into an organization's vulnerability landscape to understand the risks and helps remediation actions effectively.



A New Dimension to Cybersecurity: Continuous Vulnerability and Exposure Management (CVEM)

"Every Attacker Leverages a Weakness."

Understanding this view shifts how we approach exposure management; We MUST actively seek out weaknesses and gain a deeper understanding of our IT infrastructure. This approach leads us to go beyond exposure management, i.e., continuous vulnerability exposure management (CVEM).

Continuous Vulnerability and Exposure Management (CVEM) introduces a fresh perspective to cybersecurity by evaluating an organization's IT infrastructure security status from a Weakness Perspective and allowing it to strengthen its security posture capable of defending against cyberattacks. The weakness perspective involves the assessment of IT infrastructure that encompasses Devices, Applications, Users/ Identities, Data, Networks, and Security Controls.

To know more:
https://www.secpod.com/a-new-dimension-to-cybersecurity-continuous-vulnerability-and-exposure-management-cvem-2/

secpod

SecPod is a cyber security technology company with a mission to prevent cyberattacks on organizations. Our Advanced Vulnerability Management platform helps implement cyber hygiene measures, making it more difficult for attackers to access systems and companies' vital information.

SecPod SanerNow is a Cyber Hygiene platform providing continuous visibility to IT infrastructure. It identifies vulnerabilities, misconfigurations, and security risk exposures, mitigates loopholes to reduce the attack surface, measures compliance, and helps automate remediation. Our product philosophy is offering an easy-to-use solution with fast time-to-value that improves an organization's IT risk posture at a lower total cost of ownership vs. using point solutions.

Visit us: www.secpod.com

secpod