

Impact of Spring4shell and other Critical Vulnerabilities

Quarterly Vulnerability Report,
January to March Edition 2022

2022

January to March Edition

We are still not over the Log4J fever, and the first quarter of 2022 has already witnessed an enormous array of new vulnerabilities. **According to SecPod's security research, 6309 vulnerabilities were discovered in the first quarter of 2022, including 15 zero-days.** With the rising number of new vulnerabilities, countless threats are developed every passing day. Until we identify and remediate these vulnerabilities, the doors are wide open for attackers to invade our network. We need to battle out the most critical vulnerabilities prevalent in our network to brace against the growing cyberattacks and their ever-growing sophistication.

To boost your cyber defense skills, you need to stay on top of the latest trends in the cyber security landscape. At SecPod, we have been consistently releasing our Annual Vulnerability Report to help you manage your organization's risk exposure. To keep you equipped with next-level intelligence on vulnerabilities, we have put together a Quarterly Vulnerability Report - 2022, January to March Edition. This report will provide insights on the latest vulnerability trends and help you strategize your vulnerability management plans accordingly.

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?

1. Key Findings from SecPod's Security Research Team	04
2. Total number of vulnerabilities	05
3. Vulnerability Distribution based on CVSS v2 Severity, Exploitability Score, and Impact score	06
4. Vulnerability Distribution based on CVSS v3 Severity, 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	10
9. Top 10 Most Critical Vulnerabilities	10
10. Spring4Shell, the new Log4shell	11
11. Analytics of Malware Vulnerability Enumeration (MVE)	12
12. Vulnerability Prediction of the upcoming months using the ARIMA model	12



Key Findings from SecPod's Security Research Team

6309 is the **number of vulnerabilities discovered** between January to March 2022, which is **9.3%** more than the last three months of 2021.

As per **the CVSS v3** algorithm, **3321** vulnerabilities were reported with **critical and high severity**, **14.9% more** than the last three months of 2021.

As per **the CVSS v2** algorithm, **1446** vulnerabilities were reported with **critical and high severity**, **34.3% more** than the last three months of 2021.

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

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

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

16 of the total vulnerabilities discovered cause **High Fidelity Attacks** and are **Malware Exploiting Vulnerabilities**

65 web browser vulnerabilities were discovered in the first three months of 2022.

SecPod's Security Intelligence Coverage from January to March 2022

■ Total No of CVEs Covered: 4464

■ No of Local Checks: 3222

■ No of Remote Checks: 1242

■ Zero-day CVEs covered: 13

CVEs based on platforms:

■ Windows - 571

■ Unix - 2811

■ macOS - 351

■ Network Device Vulnerabilities: **1242**

■ Total No of Misconfigurations covered: 605

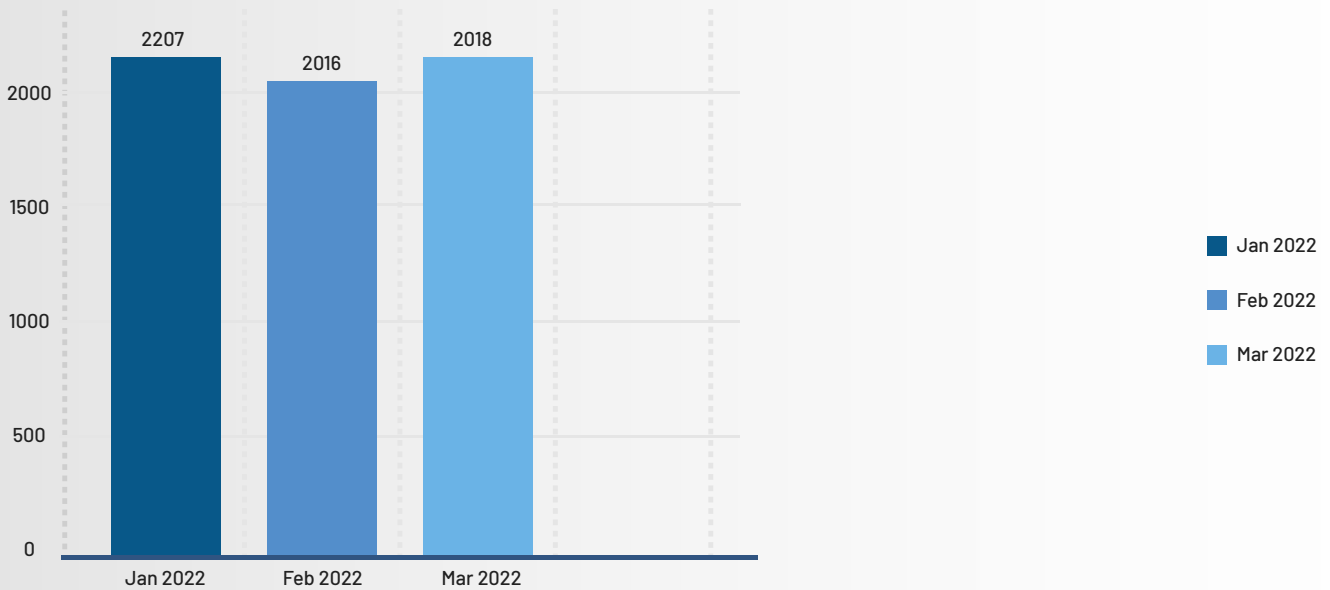
■ Total No of Third-party applications Patches Covered: 246

■ Total No of OS Patches Covered: All latest Versions for the Supported OS



Total Number of CVEs discovered

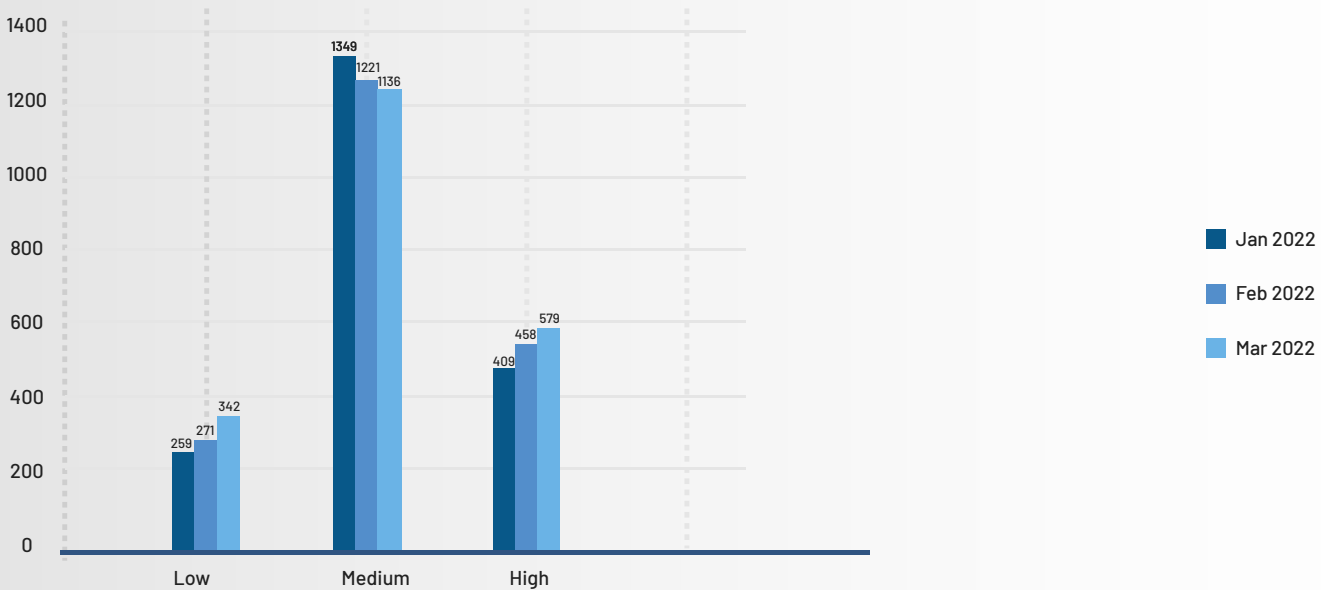
Figure 1: Shows the number of vulnerabilities published from January to March 2022.



The number of vulnerabilities published in the first three months of 2022 is 6309, 9.3% more than the 5749 vulnerabilities published in the last three months of 2021. This list includes a total of 15 zero-day vulnerabilities.

Vulnerability Severity Distribution based on CVSS v2

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

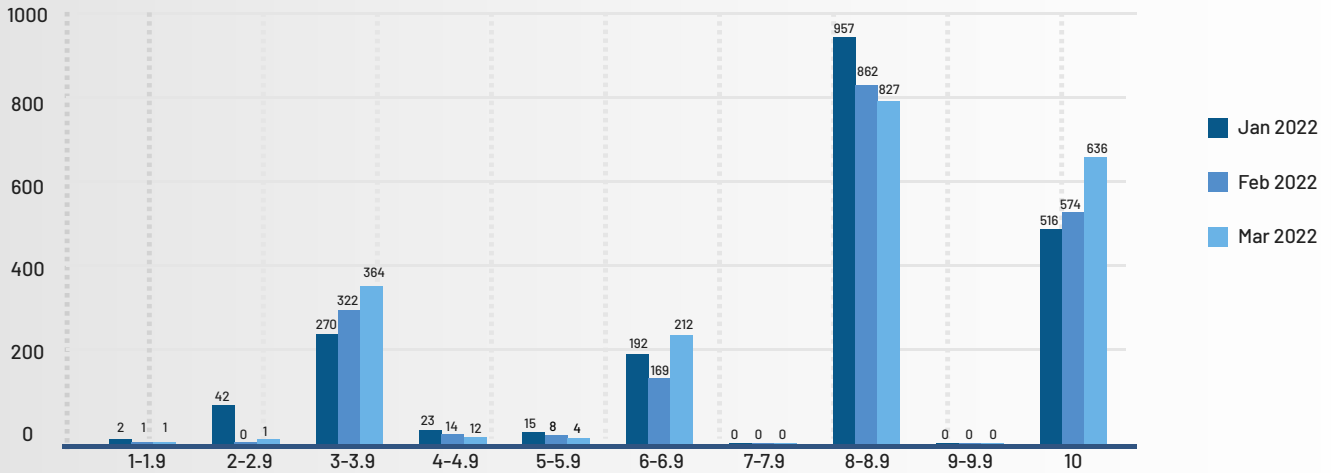


As per CVSS v2, 872 vulnerabilities were reported with low severity, 3706 vulnerabilities were reported with medium severity, and 1446 vulnerabilities were reported with high severity. An increasing trend is observed with the number of high severity vulnerabilities while comparing the monthly count.



Vulnerability Distribution based on CVSS v2 Exploitability Score

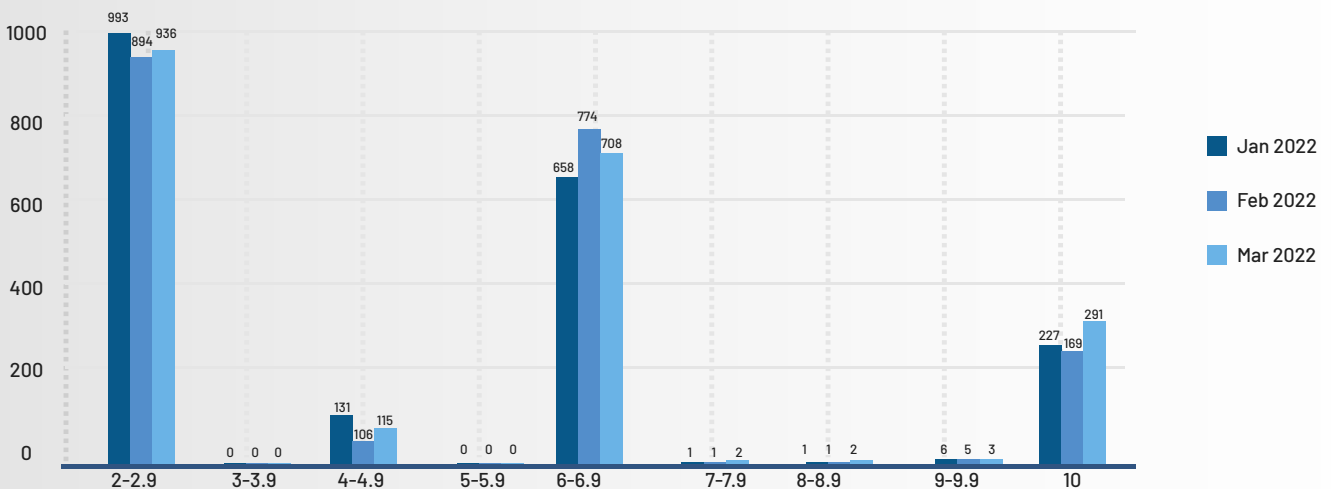
Figure 3: Depicts the distribution of vulnerabilities based on CVSS v2 exploitability score.



More vulnerabilities fall in the exploitability score of 8 – 8.9. An increasing trend is observed with the number of vulnerabilities with an exploitability score of 10, which looks critical.

Vulnerability Severity Distribution based on CVSS v2 Impact Score

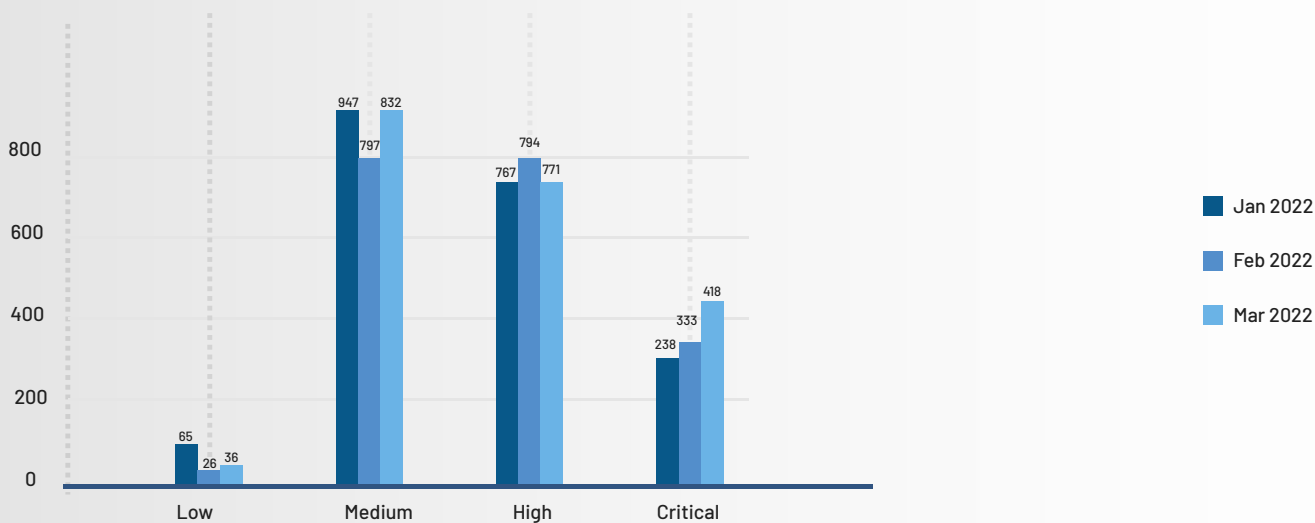
Figure 4: Depicts the distribution of vulnerabilities based on CVSS v2 impact score.



Number of vulnerabilities with the highest severity of 10 is in the increasing trend.

Vulnerability Severity Distribution based on CVSS v3

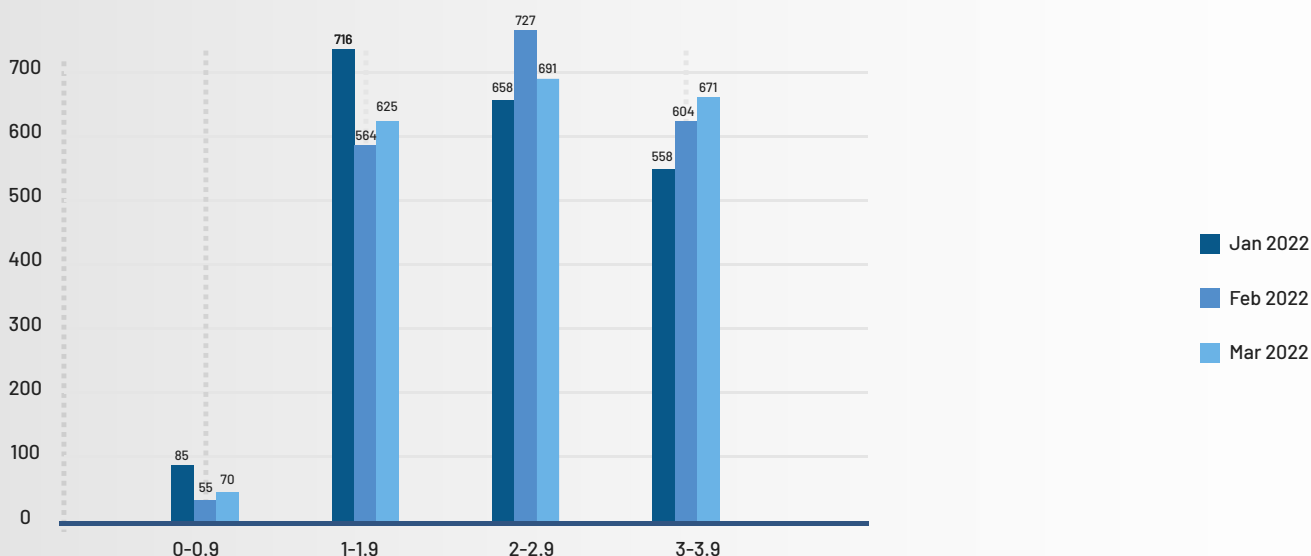
Figure 5: Depicts the vulnerability severity distribution based on CVSS v3.



As per CVSS v3, 127 vulnerabilities were reported with low severity, 2575 vulnerabilities were reported with medium severity, 2332 vulnerabilities were reported with high severity, and 989 vulnerabilities were reported critical. The total number of critical vulnerabilities is rising every month.

Vulnerability Severity Distribution based on CVSS v3 Exploitability Score

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

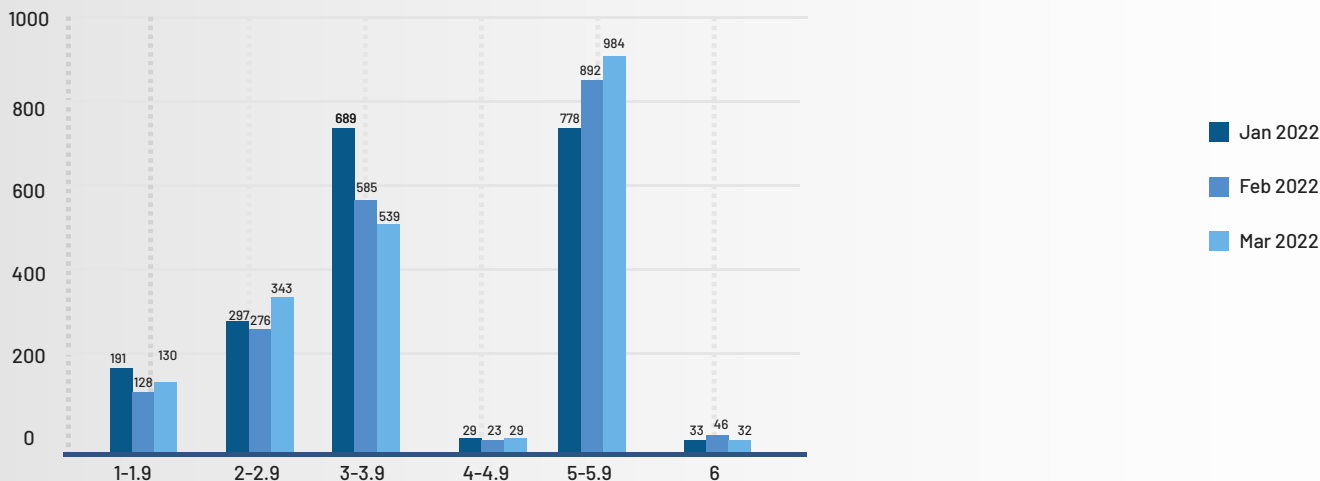


The number of vulnerabilities falling in the highest exploitability range of 3-3.9 is rising every month. More vulnerabilities are reported in the range of 2-2.9 exploitability score.



Vulnerability Severity Distribution based on CVSS v3 Impact Score

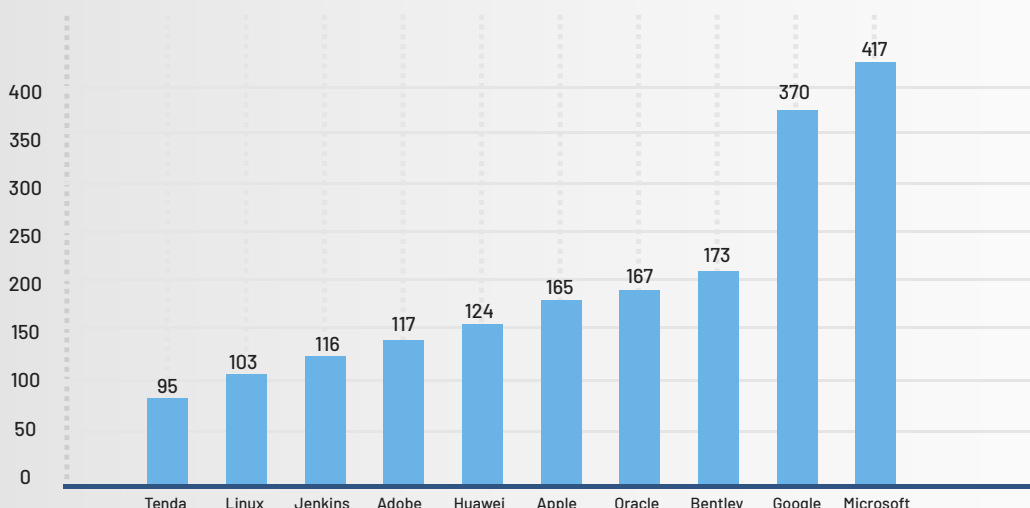
Figure 7: Depicts the distribution of vulnerabilities based on CVSS v3 impact score.



Vulnerabilities falling in the impact score between 5 to 5.9 is rising every month. More vulnerabilities are also reported in that range.

Top 10 Affected Vendors/Products

Figure 8: Shows the Top 10 vendors affected by CVEs

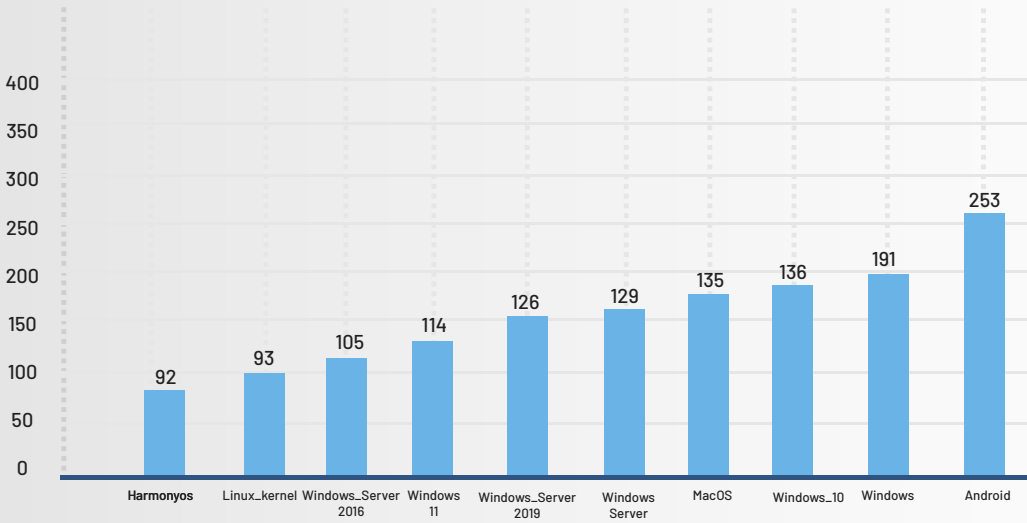


Microsoft and Google are the most affected Vendors in the first three months of 2022. Respectively they have reported 417 and 370 vulnerabilities each.



Top 10 Affected Operating Systems

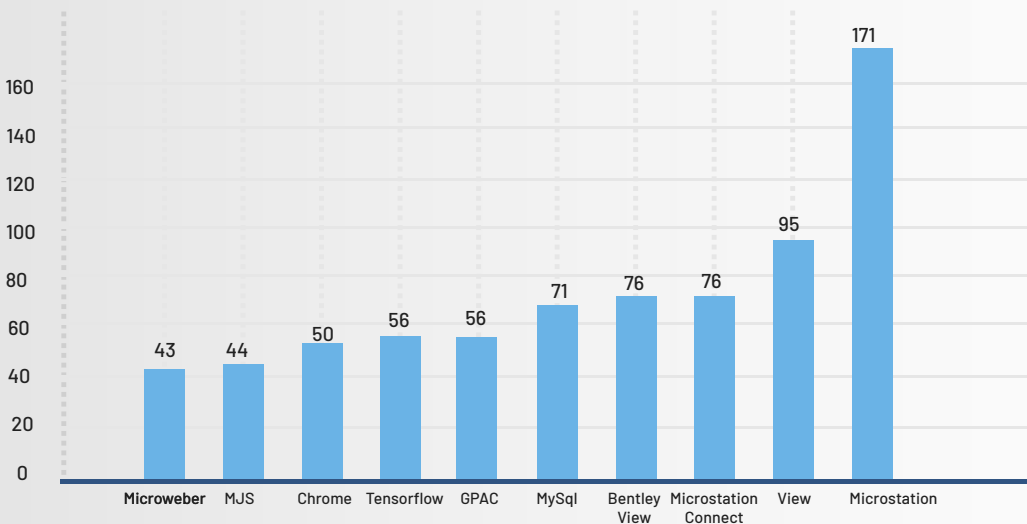
Figure 9: Shows the Top 10 Operating Systems Affected by CVEs



Android is the most affected operating system with a total of 253 vulnerabilities. Windows operating systems also reports a fair share of vulnerabilities. Mac has reported a total of 135 vulnerabilities and Linux Kernel takes a part in the list with 93 vulnerabilities.

Top 10 Affected Applications

Figure 10: Shows the Top 10 Applications Affected by CVEs

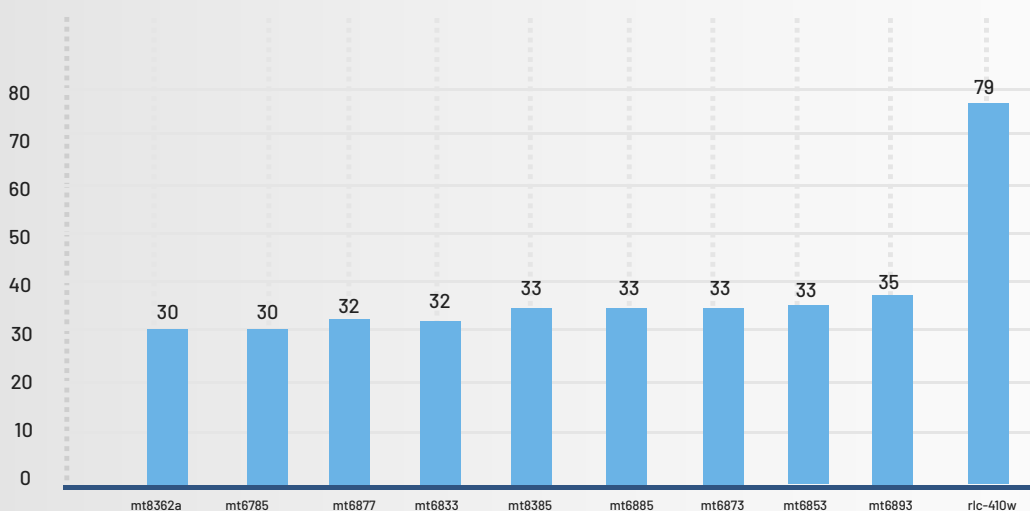


Microstation has reported the highest vulnerabilities with a total of 171. View stands second with a total of 95 vulnerabilities reported in the first 3 months of 2022.



Top 10 Affected Hardware




Figure 11: Shows the Top 10 Hardware Affected by CVEs








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 January to March 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	Product	CVSS	Impact
1	CVE-2022-21882	 Windows	7.8	A local, authenticated attacker could gain elevated local system or administrator privileges through a vulnerability in the Win32k.sys driver.
2	CVE-2022-22620	 Apple MacOS, IOS, Safari, iPadOS	8.8	WebKit Use After Free issue that could lead to OS crashes and code execution on compromised devices.
3	CVE-2022-22536	 SAP NetWeaver Application Server BAP, SAP Net Weaver Application Server Java, ABAP Platform, SAP Content Server 7.53 and SAP Web Dispatcher	10	A successful attack could result in complete compromise of Confidentiality, Integrity and Availability of the system.



4	CVE-2022-24086	 Adobe Commerce	9.8	Exploitation of this issue does not require user interaction and could result in arbitrary code execution.
5	CVE-2022-1096	 Google Chrome	9.6	Attackers can trick Chrome into running malicious code
6	CVE-2022-0847	 Linux Kernel	7.8	An unprivileged local user could use this flaw to write to pages in the page cache backed by read only files and as such escalate their privileges on the system.
7	CVE-2022-22965	 VMWare Spring Framework	9.8	An attacker can execute arbitrary code on a remote web server
8	CVE-2022-22675	 Apple iOS, MacOS	8.8	On successful exploitation, it could allow an attacker to execute code.
9	CVE-2022-26871	 Trend Micro Apex Central	9.8	Unrestricted Upload of File with Dangerous Type
10	CVE-2022-21969	 Microsoft Exchange Server	9.0	This is a Remote Code Execution Vulnerability.

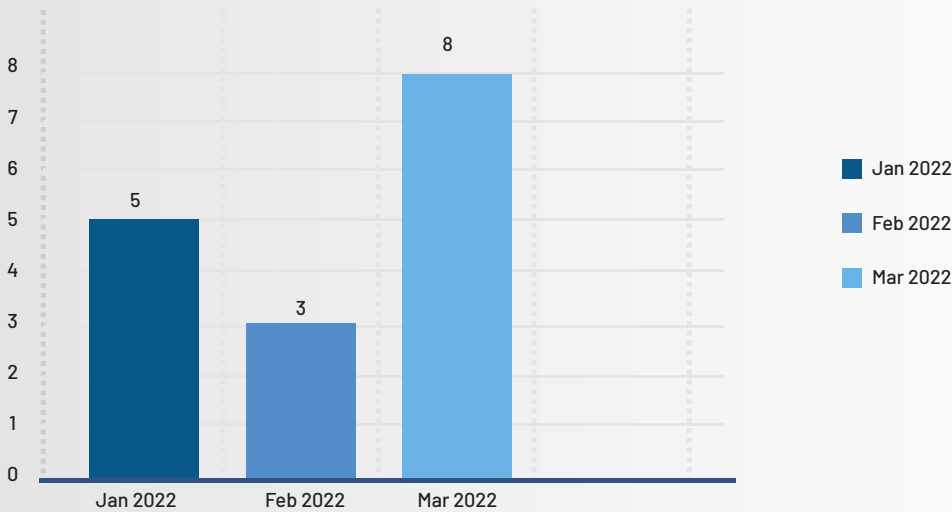
Spring4Shell (CVE-2022-22965), the new Log4shell

With many enterprises still facing the impact of Log4shell, the first three months of 2022 already witness another equivalent vulnerability, Spring4shell. This vulnerability has the potential to cause huge damage as the Log4shell vulnerability. The spring core exploit is an unauthenticated remote code execution flaw and could allow an attacker to execute code on the device remotely, that could be potentially used to deploy a malware. The Spring Developers have released the **security update** for this vulnerability in versions **5.2.20+** and **5.3.18+**. It is highly recommended to patch this vulnerability to prevent potential attacks.



Analysis on High Fidelity Attacks

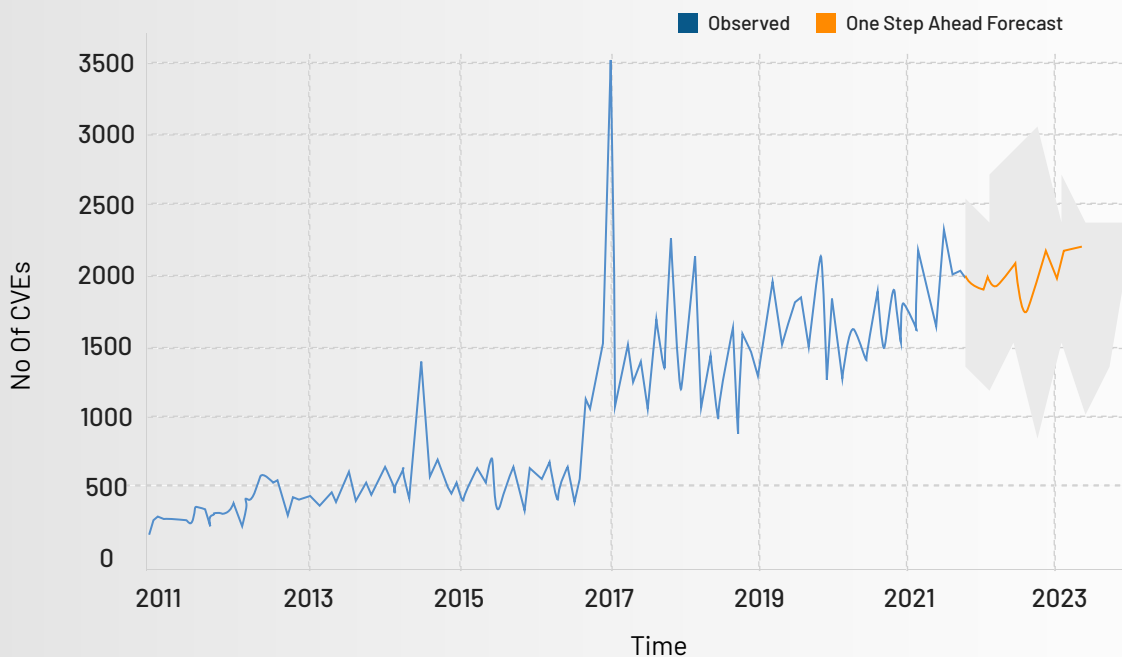
Figure 12: Depicts the monthly number of vulnerabilities that causes high fidelity attacks.



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

Vulnerability Prediction 2022

Figure 13: Displays the Vulnerability trend over the years and predicts the vulnerability count for 2022



On observing the vulnerability trend over the years, from SecPod we predict over 25000 vulnerabilities in 2022. This prediction is made based on the ARIMA (Autoregressive Integrated Moving Average) model.

SecPod SanerNow Advanced Vulnerability Management for the Growing Vulnerability Landscape

Based on SecPod's security research, 20150 is the number of vulnerabilities discovered in 2021, with an average of 50 - 60 vulnerabilities per day. The growing rise in the number of vulnerabilities is here to stay. Attackers will look out for these loopholes and invent more sophisticated ways to invade our IT network. SecPod SanerNow provides an advanced vulnerability management solution to deal with vulnerabilities and security risks beyond them. With SanerNow, you can perform continuous and automated vulnerability management leveraging our homegrown world's largest vulnerability intelligence feed with 160,000+ security checks. SanerNow enables you to run the industry's fastest scan to identify the vulnerabilities in less than 5 minutes and quickly remediate them with our integrated patch management.

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

Call us at:

India - (+91) 80 4121 4020 /

USA - (+1) 918 625 3023

www.secpod.com