Gattrix

SECURITY INTELLIGENCE ADVISORY

01st Jan 2024 – 31st Jan 2024

INTENT

This report is intended to help quantify the scope of the risks as organizations struggle to balance their cyber security policies and protections against the needs of their employees for access to the Web and its resources.

BACKGROUND

Every organization, large, medium, or small, faces the significant challenge of managing vulnerabilities present in the operating systems. Unattended vulnerabilities pose a severe threat to your organization. They can expose you to various threats, including threats from users within the system, competitors seeking to gain access to sensitive information, etc. It is crucial to identify such vulnerabilities and apply updates and patches to remediate them and mitigate potential associated risks.

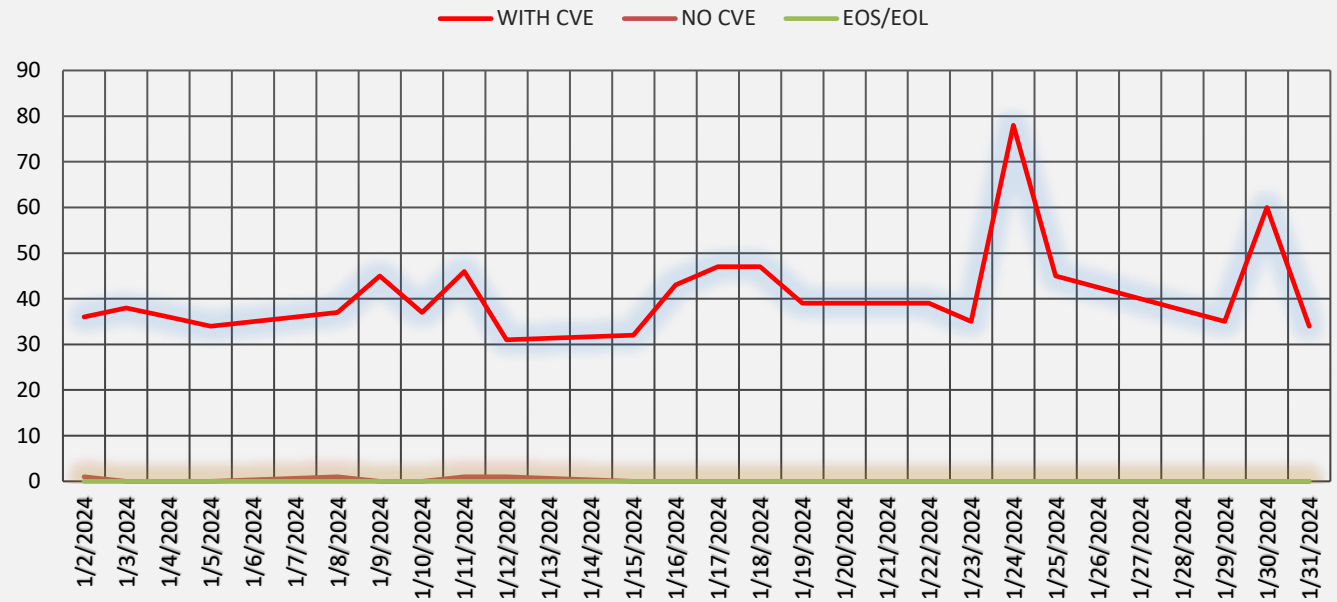
One effective way to stay on top of these vulnerabilities is by conducting regular vulnerability assessments. These periodic assessments cover your entire IT infrastructure and help you identify new threats that may have emerged. This proactive practice enables you to stay abreast of the current state of your security posture and helps you keep your organization safe and secure.

WHAT DOES THE VULNERABILITY ADVISORY COVER?

- We monitor around 2000 applications, appliances, and operating systems and test and verify the vulnerabilities reported in them.
- We focus on each vulnerability disclosed in these 2000 products.
- The systems and applications monitored by the Sattrix Research Team are those in use in the customers' environment.
- If customers use products that aren't already being monitored by our team, they can be submitted to us, and we will initiate monitoring them the next business day. We only monitor public or commercially available solutions.
- The Vulnerability Database covers vulnerabilities that can be exploited in all types of products – software, hardware, firmware, etc.
- The vulnerabilities verified by our team are described in the client database as an Advisory and listed in the Sattrix Vulnerability Reports, detailing what IT Security teams need to know to mitigate the risk posed by the vulnerability in their environment.
- The Vulnerability Database covers vulnerabilities that can be exploited in all types of products. We also cover zero days and eos/eol.
- We create daily and weekly reports covering all the details about detected vulnerabilities and the total vulnerability count in the last week and provide them to customers.
- The Sattrix Advisory descriptions include severity, under investigation product, Affected Product, CVE ID, Sattrix score, reference links, and remediation recommendations.
- Sattrix researchers complete the vulnerability assessment process within 5 business working days.

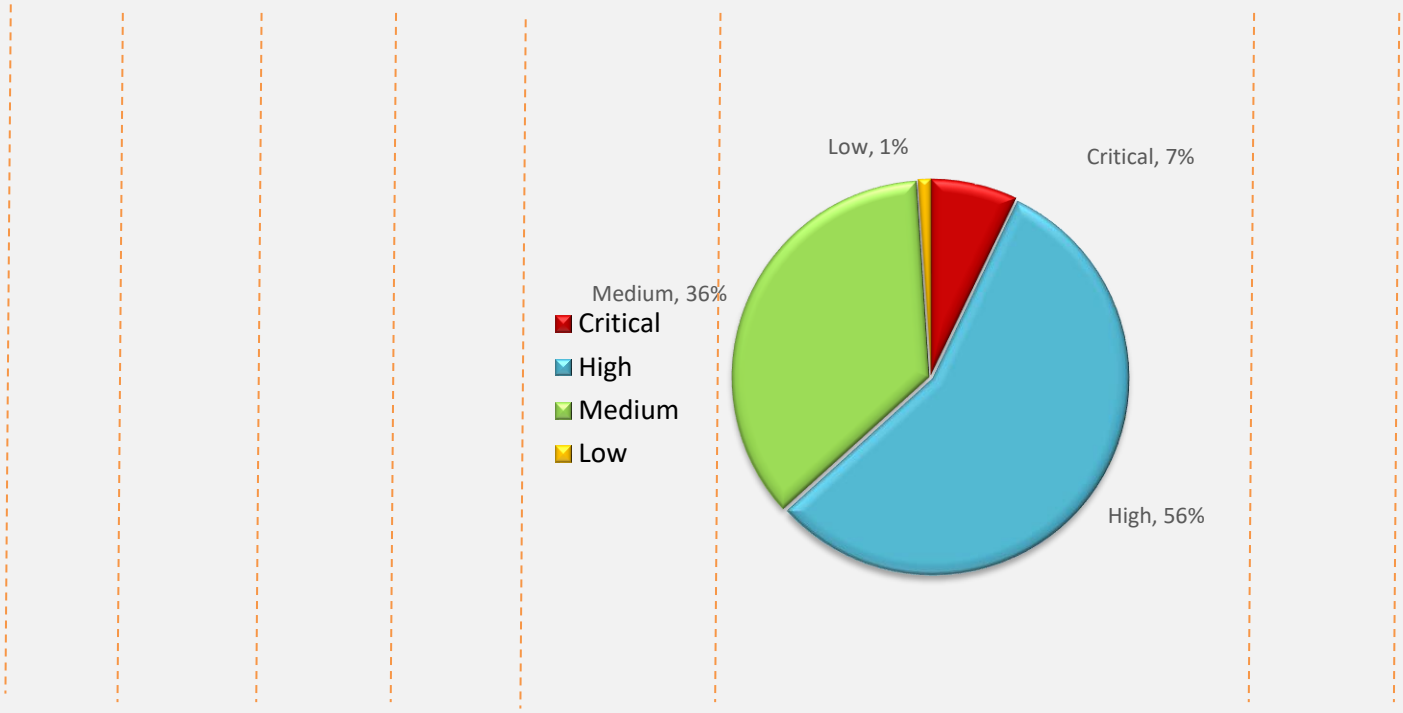
EXECUTIVE SUMMARY

Overall Monthly Vulnerability Trend Chart



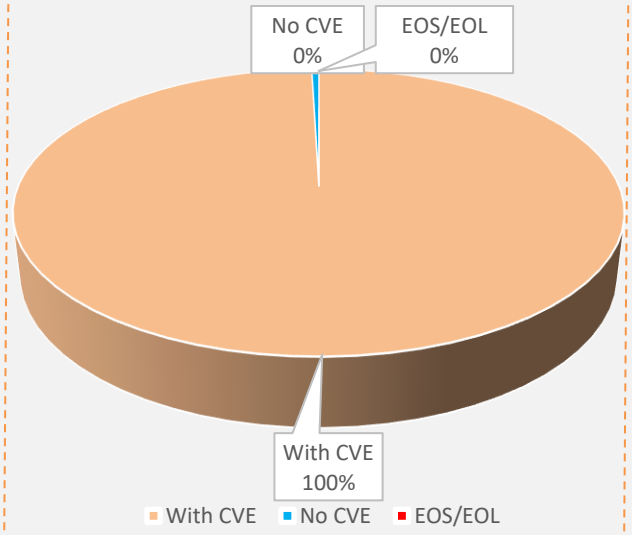
Released Vulnerabilities and Severity Count:

This graph presents threat levels based on vulnerability identified.

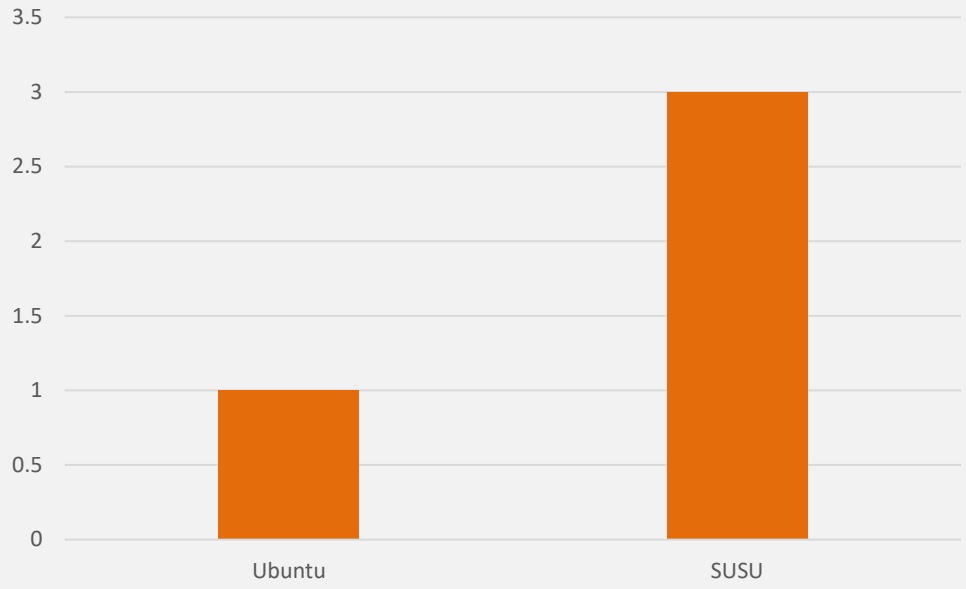


EXECUTIVE SUMMARY

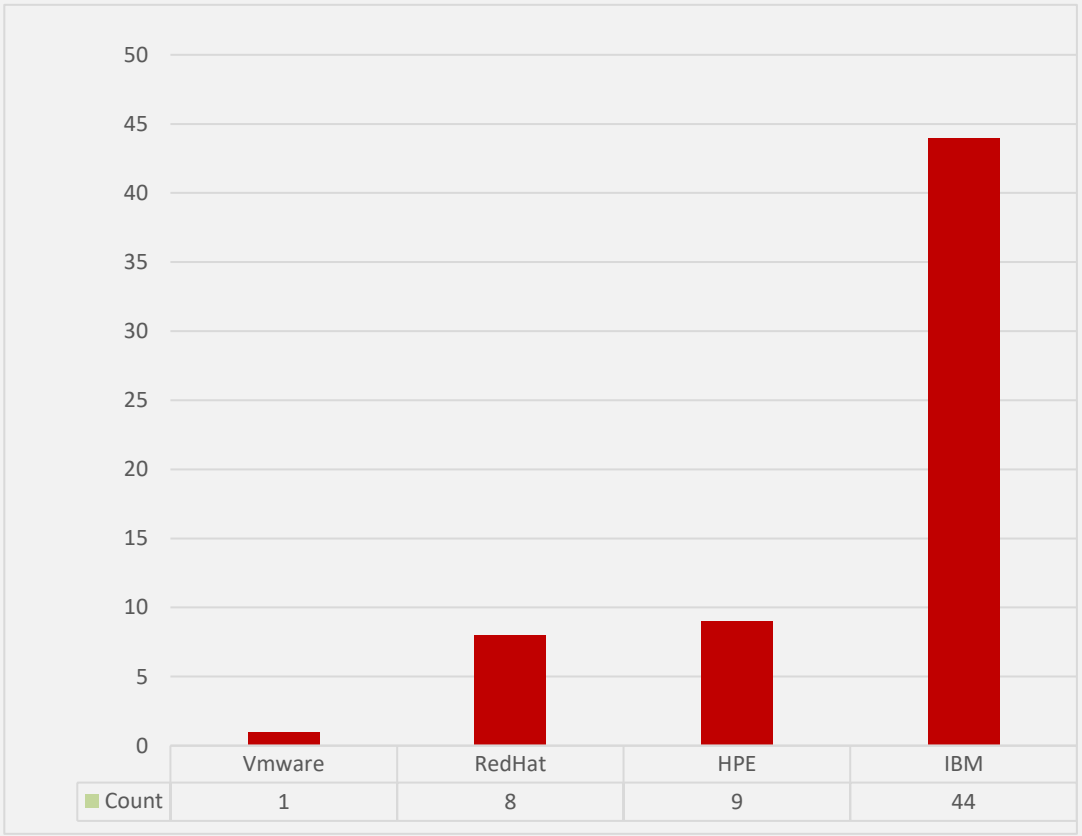
This graph presents the total vulnerabilities released, including zero-day vulnerability and EOS/EOL, with their count.



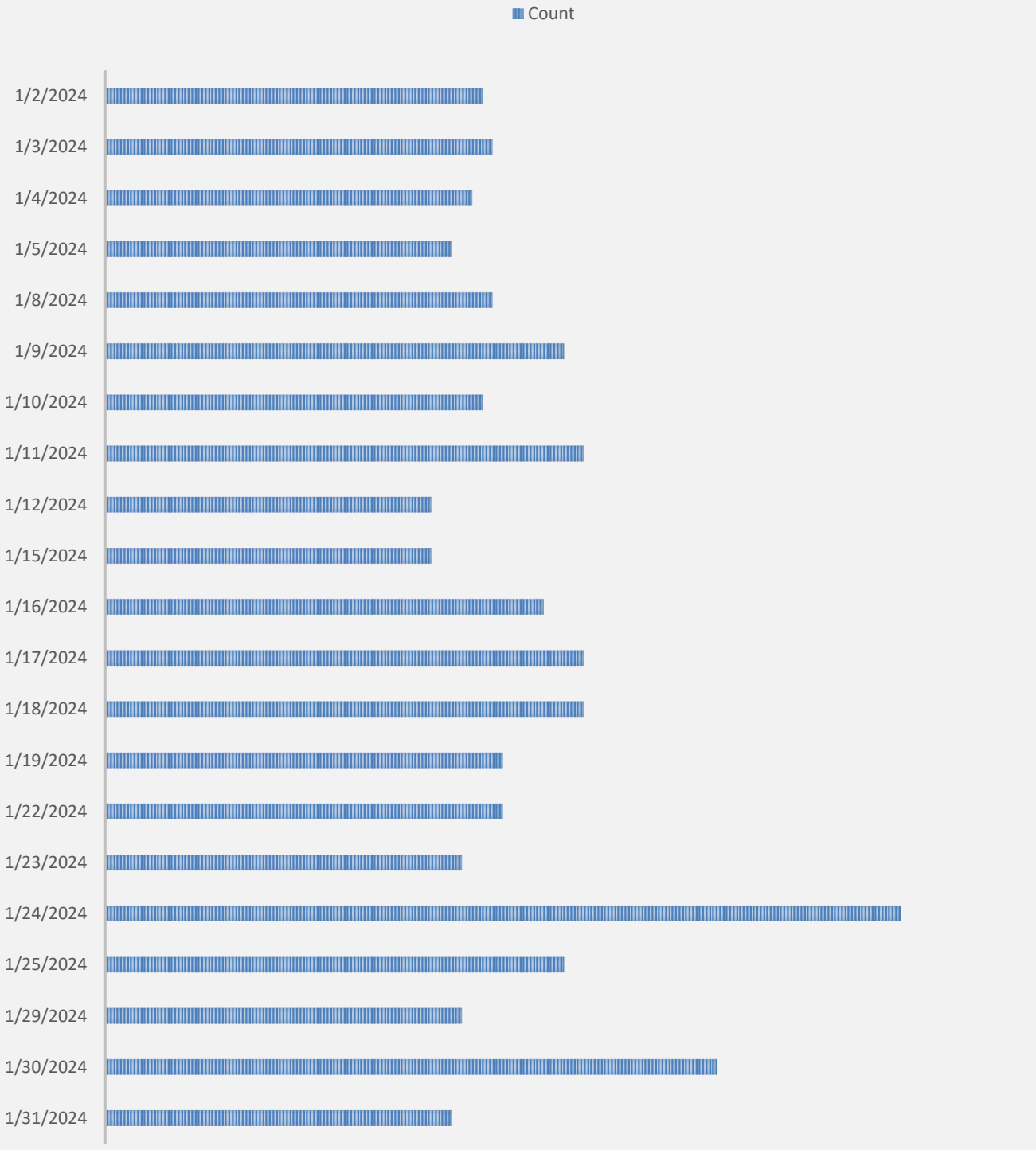
Product-wise Released Non-CVE ID or Zero Day Vulnerabilities Count



Critical CVE Count

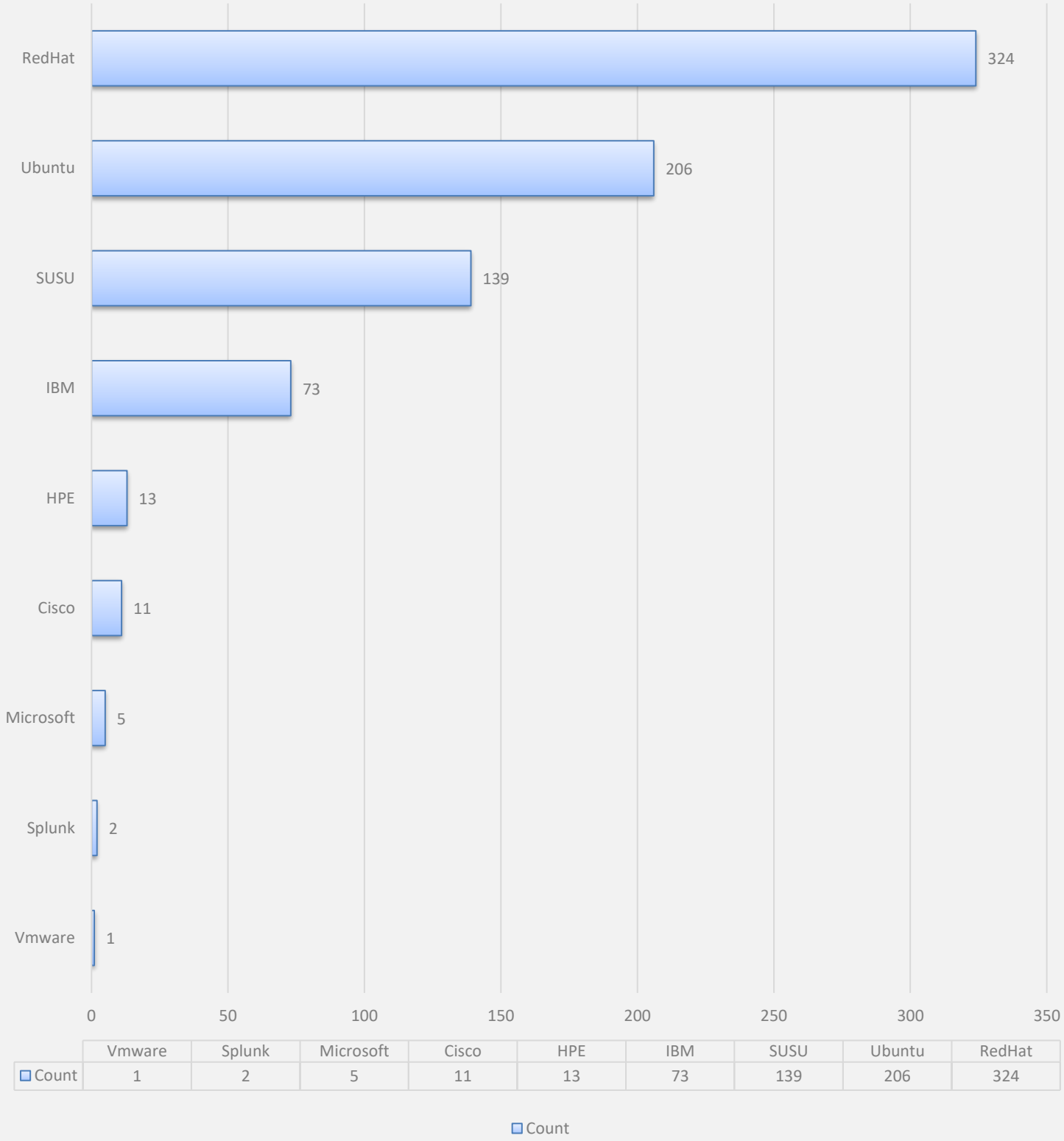


Date-wise Released Vulnerabilities Count, Fortnightly Summarized



	1/31/2024	1/30/2024	1/29/2024	1/25/2024	1/24/2024	1/23/2024	1/22/2024	1/19/2024	1/18/2024	1/17/2024	1/16/2024	1/15/2024	1/12/2024	1/11/2024	1/10/2024	1/9/2024	21/8/2024	21/5/2024	21/4/2024	21/3/2024	21/2/2024
Count	34	60	35	45	78	35	39	39	47	47	43	32	32	47	37	45	38	34	36	38	37

Product-wise Chart for CVE



	Vmware	Splunk	Microsoft	Cisco	HPE	IBM	SUSU	Ubuntu	RedHat
Count	1	2	5	11	13	73	139	206	324

TOP VULNERABILITIES OF THE MONTH

DATE	CVE ID	Vendor	Summary	Recommendation
05-01-24	CVE-2022-46892 CVE-2022-37459 CVE-2021-45454 CVE-2022-32295 CVE-2022-25368"	HPE	HPE ProLiant RL300 Gen11 Servers Using Ampere BIOS, Multiple Vulnerabilities	Updates available; please see the reference link below: https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04587en_us
15-01-24	CVE-2020-7692 CVE-2021-22573	IBM	Here is a vulnerability in google-oauth-client-1.25.0.jar used by IBM Maximo Manage application in IBM Maximo Application Suite	Updates available; please see the reference link below: https://www.ibm.com/support/pages/node/7107713
15-01-24	CVE-2021-42581	IBM	IBM Storage Ceph is vulnerable to Prototype Pollution in Ramda [CVE-2021-42581]	Updates available; please see the reference link below: https://www.ibm.com/support/pages/node/7107781
16-01-24	CVE-2019-25033 CVE-2022-3094 CVE-2022-35205 CVE-2022-35206 CVE-2022-48468 CVE-2023-22745 CVE-2023-36049 CVE-2023-36558	IBM	Multiple security vulnerabilities affect IBM Robotic Process Automation for Cloud Pak.	Updates available; please see the reference link below: https://www.ibm.com/support/pages/node/7107897
18-01-24	CVE-2023-3446 CVE-2023-3817 CVE-2023-5678 CVE-2023-5981 CVE-2023-7104 CVE-2023-39615 CVE-2023-49568 CVE-2023-49569	RedHat	Red Hat Advanced Cluster Management 2.9.2 security and bug fix container updates	Updates available; please see the reference link below: https://access.redhat.com/errata/RHSA-2024:0298
23-01-24	CVE-2023-34063	Vmware	VMware Aria Automation (formerly vRealize Automation) updates address a Missing Access Control vulnerability"	Updates available; please see the reference link below: https://www.vmware.com/security/advisories/VMSA-2024-0001.html
29-01-24	CVE-2021-40438 CVE-2023-50274 CVE-2023-50275 CVE-2023-6573	HPE	HPE OneView, Multiple Vulnerabilities	Updates available; please see the reference link below: https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04586en_us

Global Presence

USA / Sattrix Information Security Incorporation
UK/EU / Sattrix Info Security Ltd
MEA / Sattrix Information Security DMCC
India / Sattrix Information Security (P) Ltd

Office Address
1 Parklane Blvd, Ste 729 E;
Dearborn, MI 48126

Global SOC
516, 517 Shivalik Shilp,
ISON Cross Road, S G Highway, Ahmedabad

+1 416-917-8344 **info@sattrix.com** **www.sattrix.com**