Gattrix™

SECURITY INTELLIGENCE ADVISORY

01st Mar 2024 – 31st Mar 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.

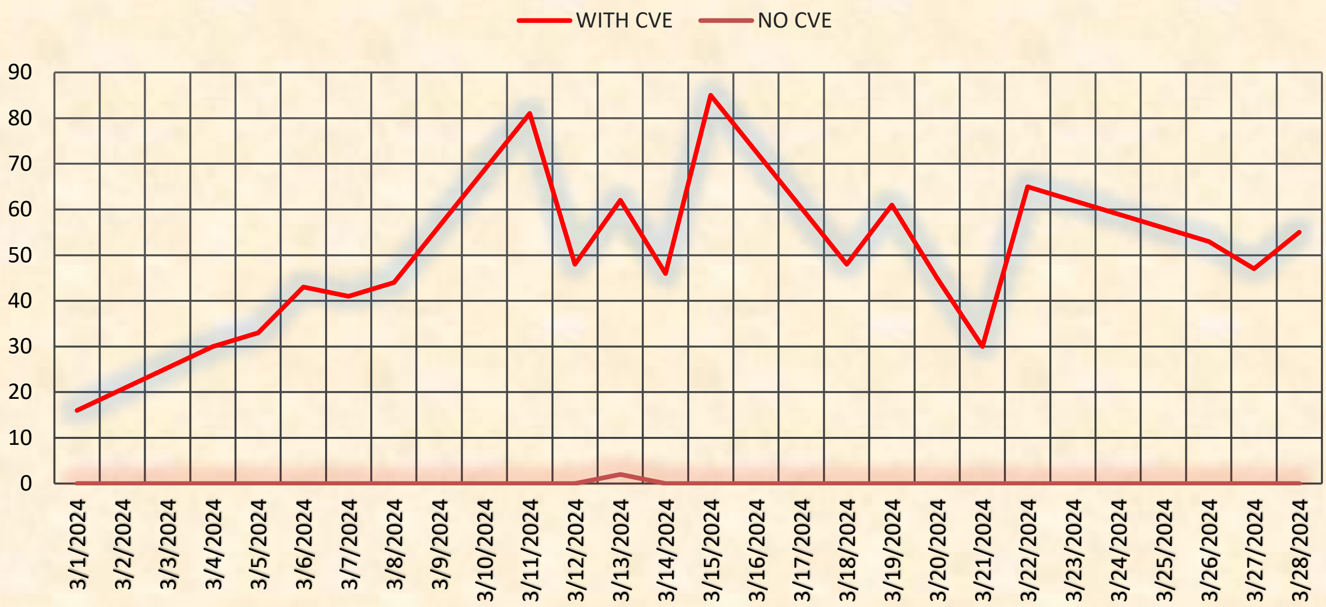
One effective way to stay on top of these vulnerabilities is by conducting regular vulnerability assessments. These periodic assessments cover your entire IT infrastructure and help you identify new threats that may have emerged. This proactive practice enables you to stay abreast of the current state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

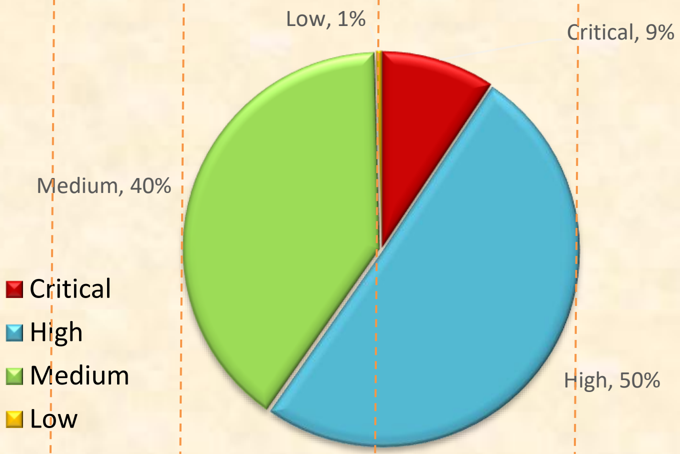
EXECUTIVE SUMMARY

Overall Monthly Vulnerability Trend Chart



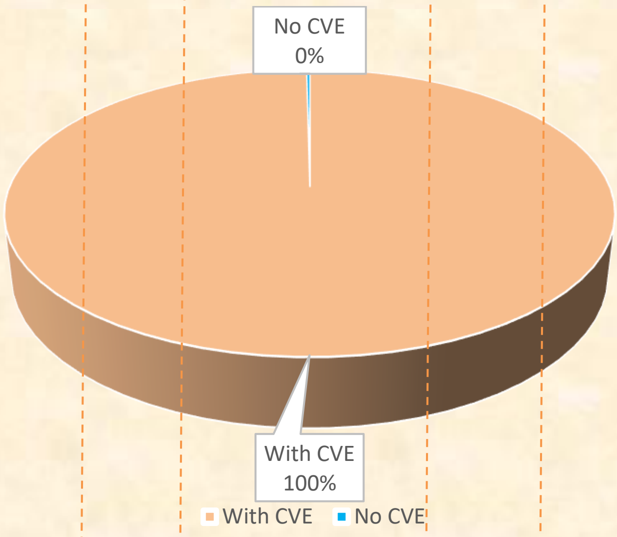
Released Vulnerabilities and Severity Count:

This graph presents threat levels based on vulnerability identified.

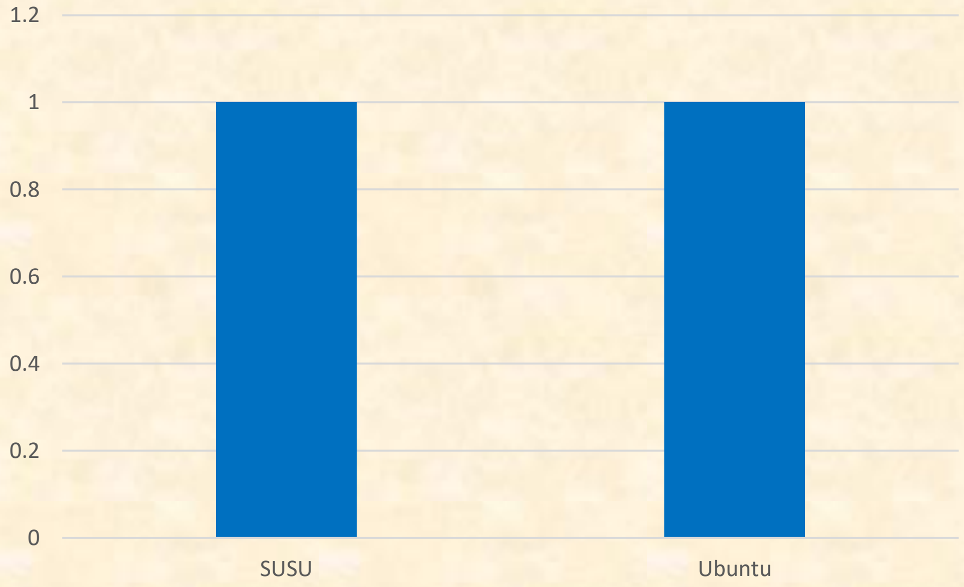


EXECUTIVE SUMMARY

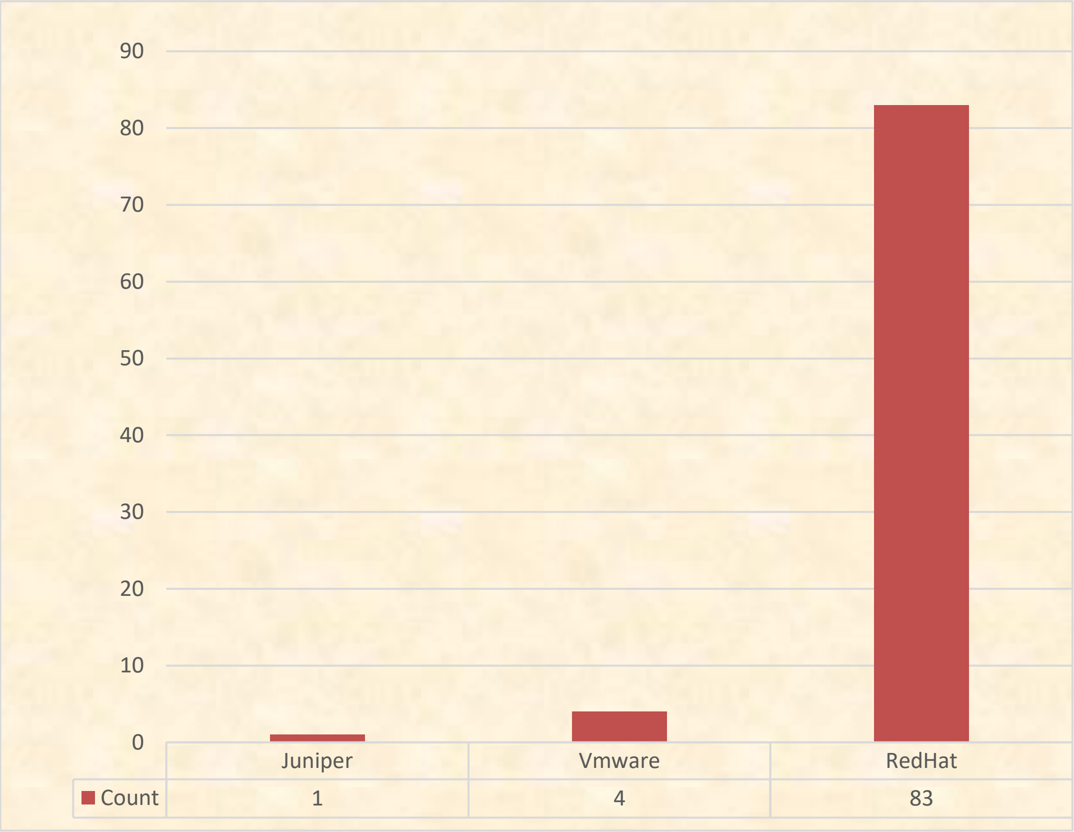
This graph presents the total vulnerabilities released, including zero-day vulnerability with their count.



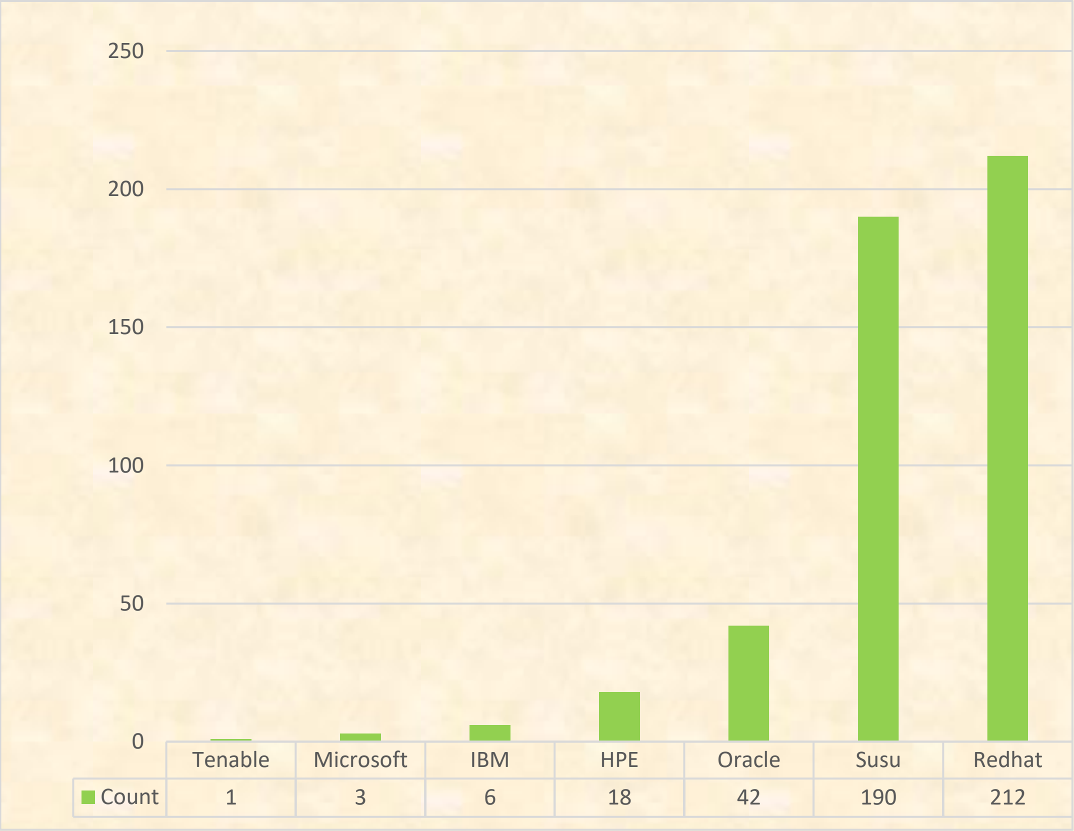
Product-wise Released Non-CVE ID or Zero Day Vulnerabilities Count



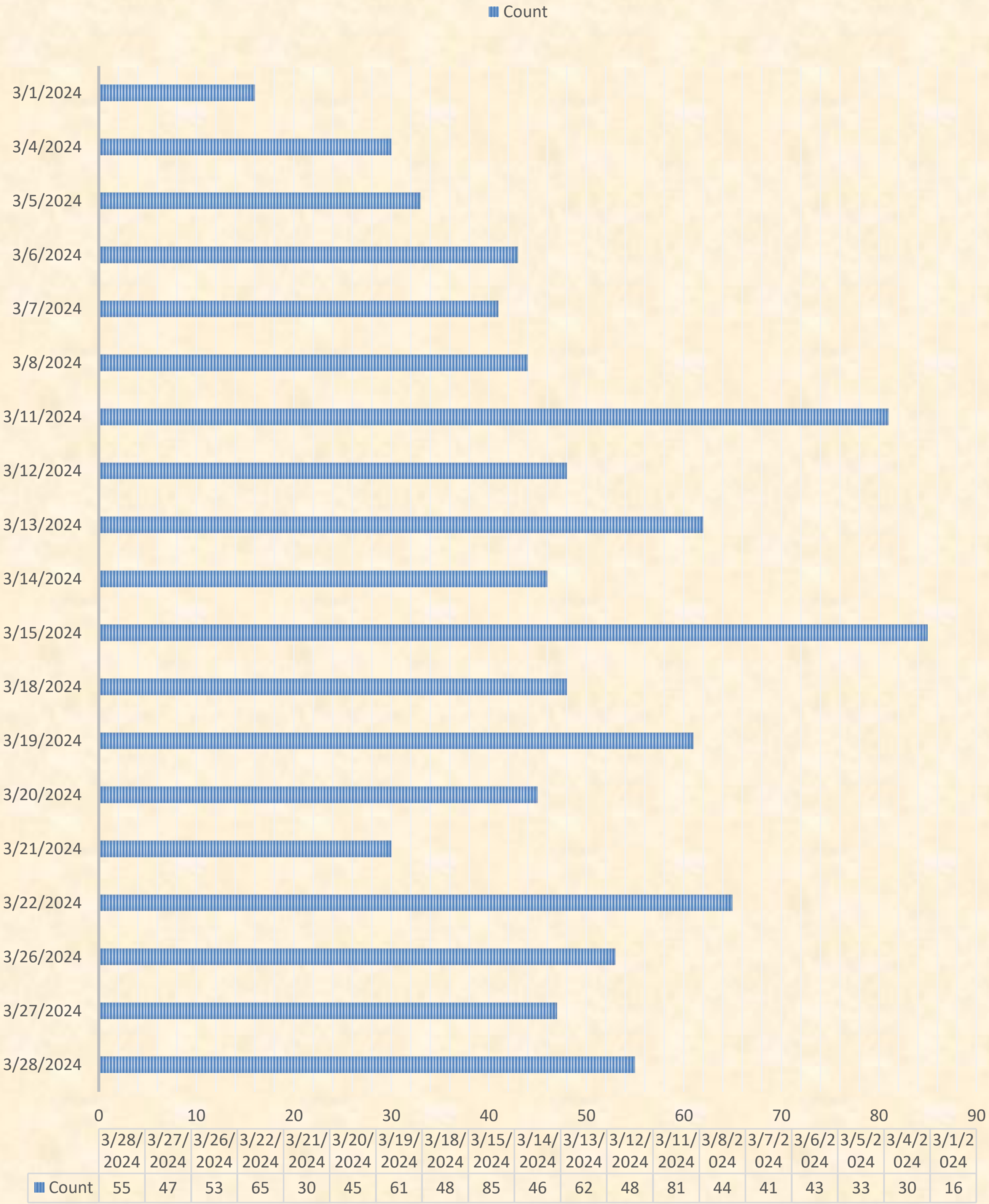
Critical CVE Count :-



HIGH CVE Count :-

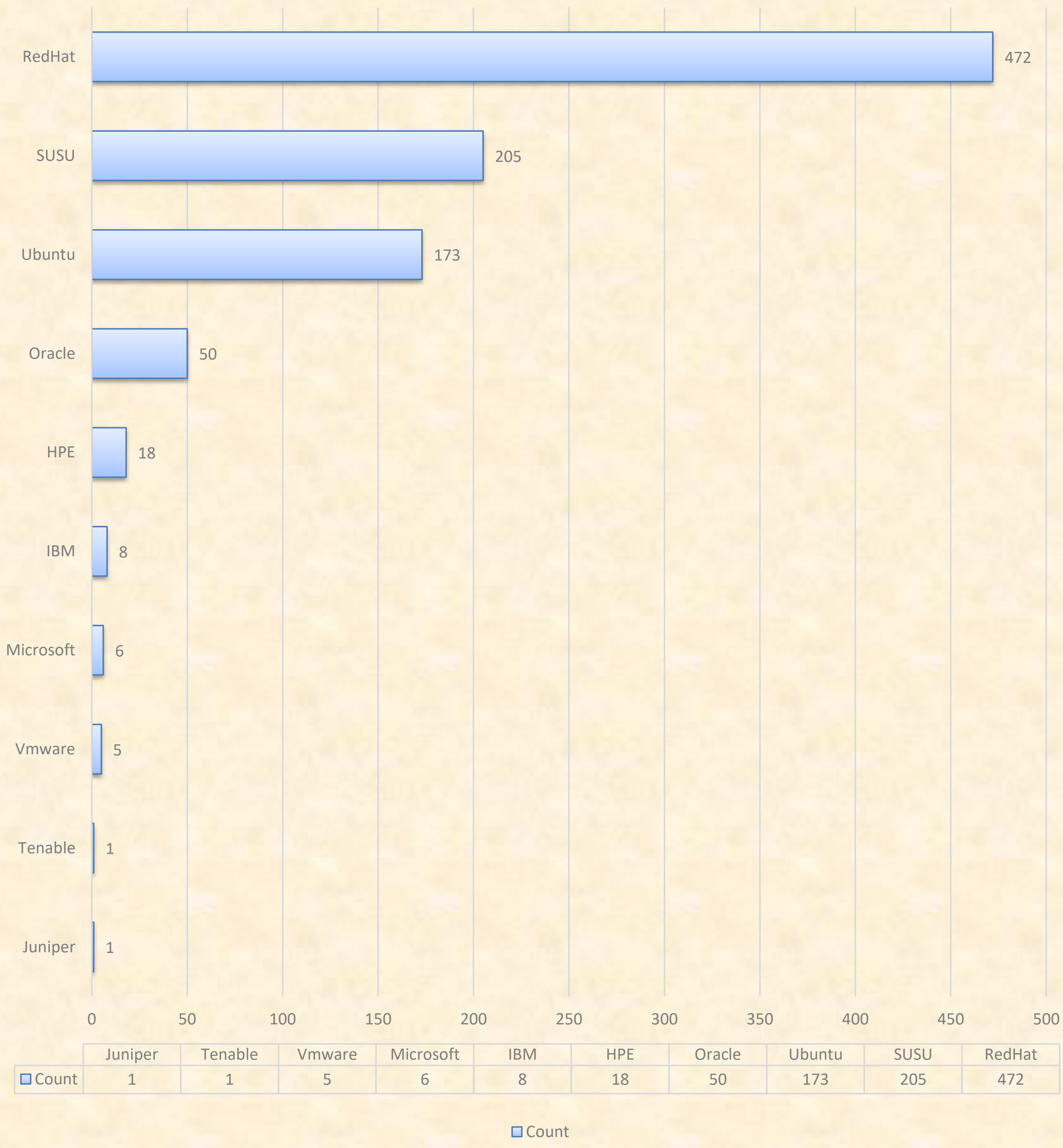


Date-wise Released Vulnerabilities Count, Fortnightly Summarized



	3/28/2024	3/27/2024	3/26/2024	3/22/2024	3/21/2024	3/20/2024	3/19/2024	3/18/2024	3/15/2024	3/14/2024	3/13/2024	3/12/2024	3/11/2024	3/8/2024	3/7/2024	3/6/2024	3/5/2024	3/4/2024	3/1/2024
▥ Count	55	47	53	65	30	45	61	48	85	46	62	48	81	44	41	43	33	30	16

Product-wise Chart for CVE



	Juniper	Tenable	Vmware	Microsoft	IBM	HPE	Oracle	Ubuntu	SUSU	RedHat
□ Count	1	1	5	6	8	18	50	173	205	472

TOP VULNERABILITIES OF THE MONTH

DATE	CVE ID	Vendor	Summary	Recommendation
05-03-24	CVE-2024-22252 CVE-2024-22253 CVE-2024-22254 CVE-2024-22255	Vmware	VMware ESXi, Workstation, and Fusion updates address multiple security vulnerabilities	Updates are available please see below reference link: https://www.vmware.com/security/advisories/VMSA-2024-0006.html
06-03-24	CVE-2023-49568 CVE-2023-49569 CVE-2023-50387 CVE-2023-50868 CVE-2023-51042 CVE-2023-51043 CVE-2024-0193 CVE-2024-1085 CVE-2024-1086	RedHat	OpenShift Container Platform 4.12.51 bug fix and security update	Updates are available please see below reference link: https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04604en_us
09-03-24	CVE-2024-21591	Juniper	Junos OS: SRX Series and EX Series: Security Vulnerability in J-web allows a preAuth Remote Code Execution	Updates are available please see below reference link: https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Junos-OS-SRX-Series-and-EX-Series-Security-Vulnerability-in-J-web-allows-a-preAuth-Remote-Code-Execution-CVE-2024-21591?language=en_US
12-03-24	CVE-2023-42465	SUSU	Security update for sudo	Updates are available please see below reference link: https://www.suse.com/support/update/announcement/2024/suse-su-20240834-1/
14-03-24	CVE-2024-2390	Tenable	Tenable Plugin Feed ID #202403142053 Fixes Privilege Escalation Vulnerability	Updates are available please see below reference link: https://www.tenable.com/security/tns-2024-05
18-03-24	CVE-2024-26190	Microsoft	Microsoft QUIC Denial of Service Vulnerability	Updates are available please see below reference link: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-26190
19-03-24	CVE-2022-4886	IBM	Kubernetes ingress-nginx information disclosure	Updates are available please see below reference link: https://www.ibm.com/support/pages/node/7116638
26-03-24	CVE-2024-22436	HPE	HPE IceWall Products, Remote Denial of Service (DoS)	Updates are available please see below reference link: https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbmu04626en_us

Disclaimer: The information in this document is subject to change without notice and should not be construed as a commitment by Sattrix Information Security (P) Ltd. Sattrix provides no warranty, express or implied, including warranties of merchantability and information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall Sattrix or any of its suppliers be liable for direct, indirect, special, incidental, or consequential damages of any nature or kind arising from the use of this document or the use of any hardware or software described in this document, even if Sattrix or its suppliers have been advised of the possibility of such damages. This document and parts hereof must not be reproduced or copied without written permission from Sattrix, and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose. All rights to registrations and trademarks reside with their respective owners

Limitation of Liability: IN NO EVENT SHALL Sattrix, Sattrix AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD-PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF Sattrix HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Global Presence

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

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

India Office Address
28, Damubhai Colony,
Anjali Cross Roads,
Ahmedabad - 380007

+91 796 819 6800 info@sattrix.com www.sattrix.com