Gattrix

SECURITY INTELLIGENCE ADVISORY

01st Feb 2024 – 29th Feb 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.

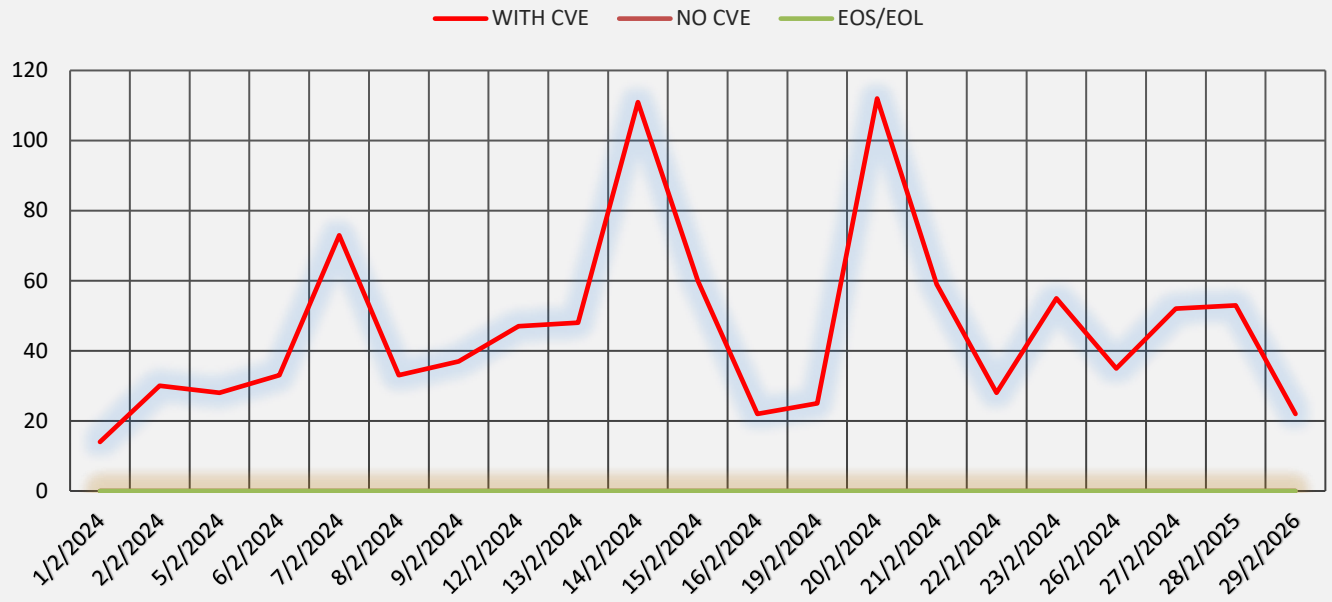
One effective way to stay on top of these vulnerabilities is by conducting regular vulnerability assessments. These periodic assessments cover your entire IT infrastructure and help you identify new threats that may have emerged. This proactive practice enables you to stay abreast of the current state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

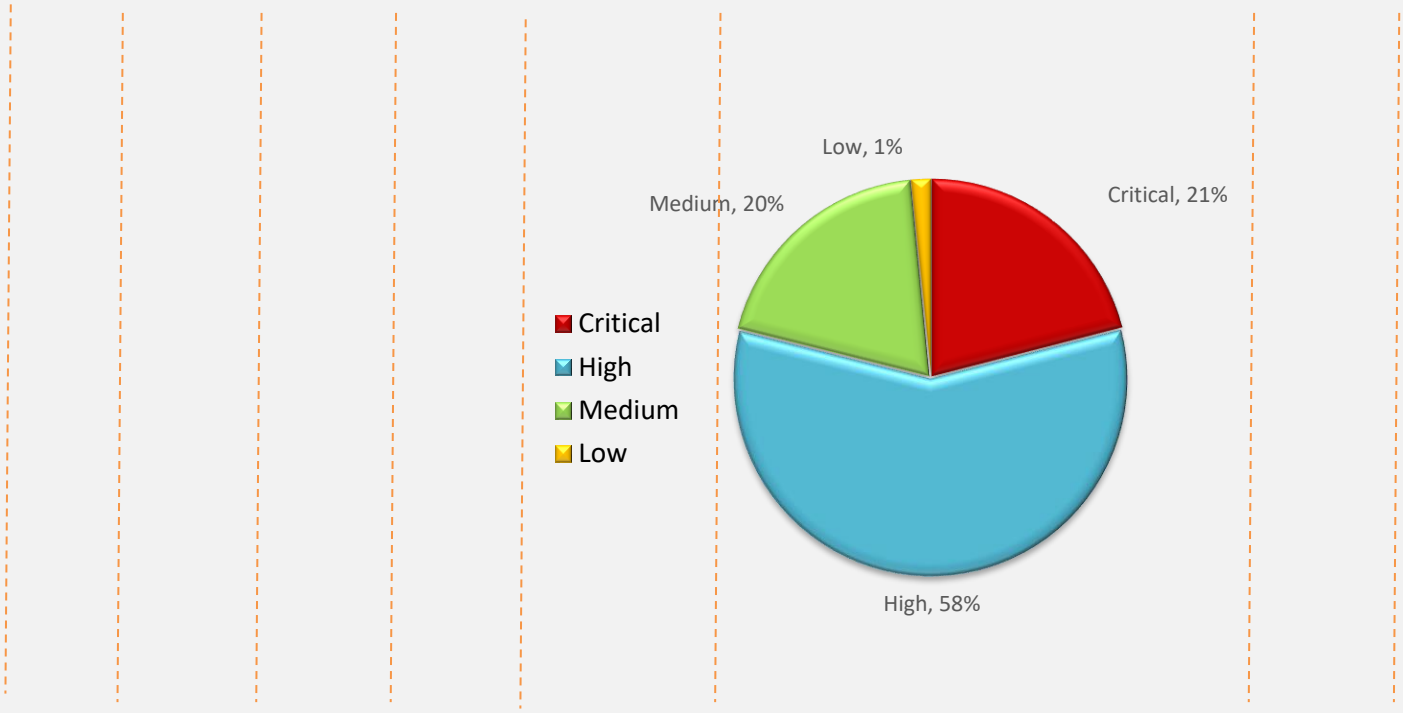
EXECUTIVE SUMMARY

Overall Monthly Vulnerability Trend Chart



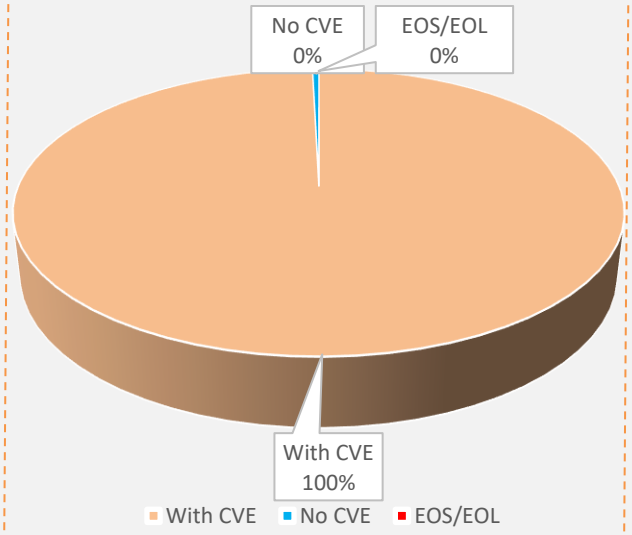
Released Vulnerabilities and Severity Count:

This graph presents threat levels based on vulnerability identified.

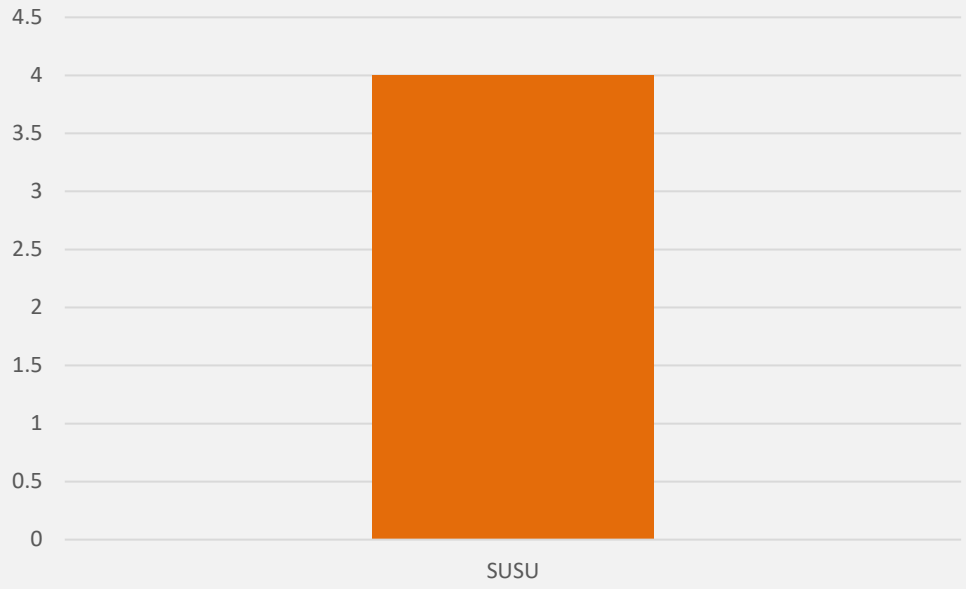


EXECUTIVE SUMMARY

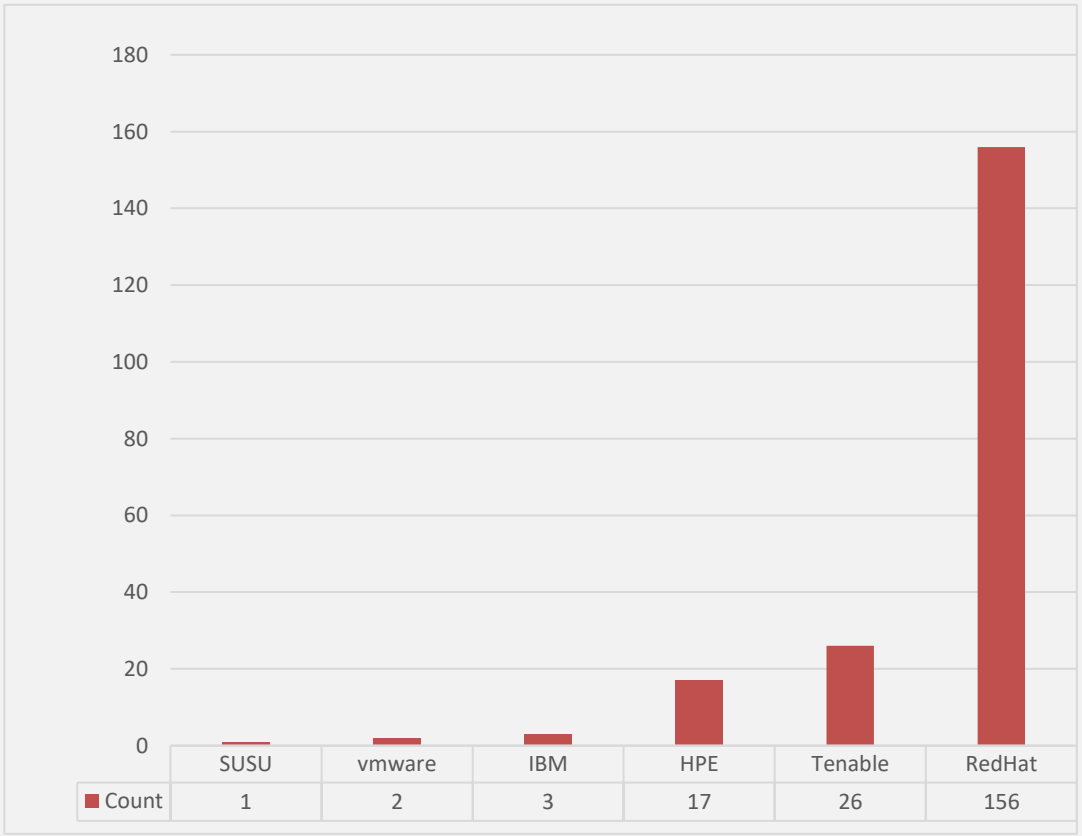
This graph presents the total vulnerabilities released, including zero-day vulnerability and EOS/EOL, with their count.



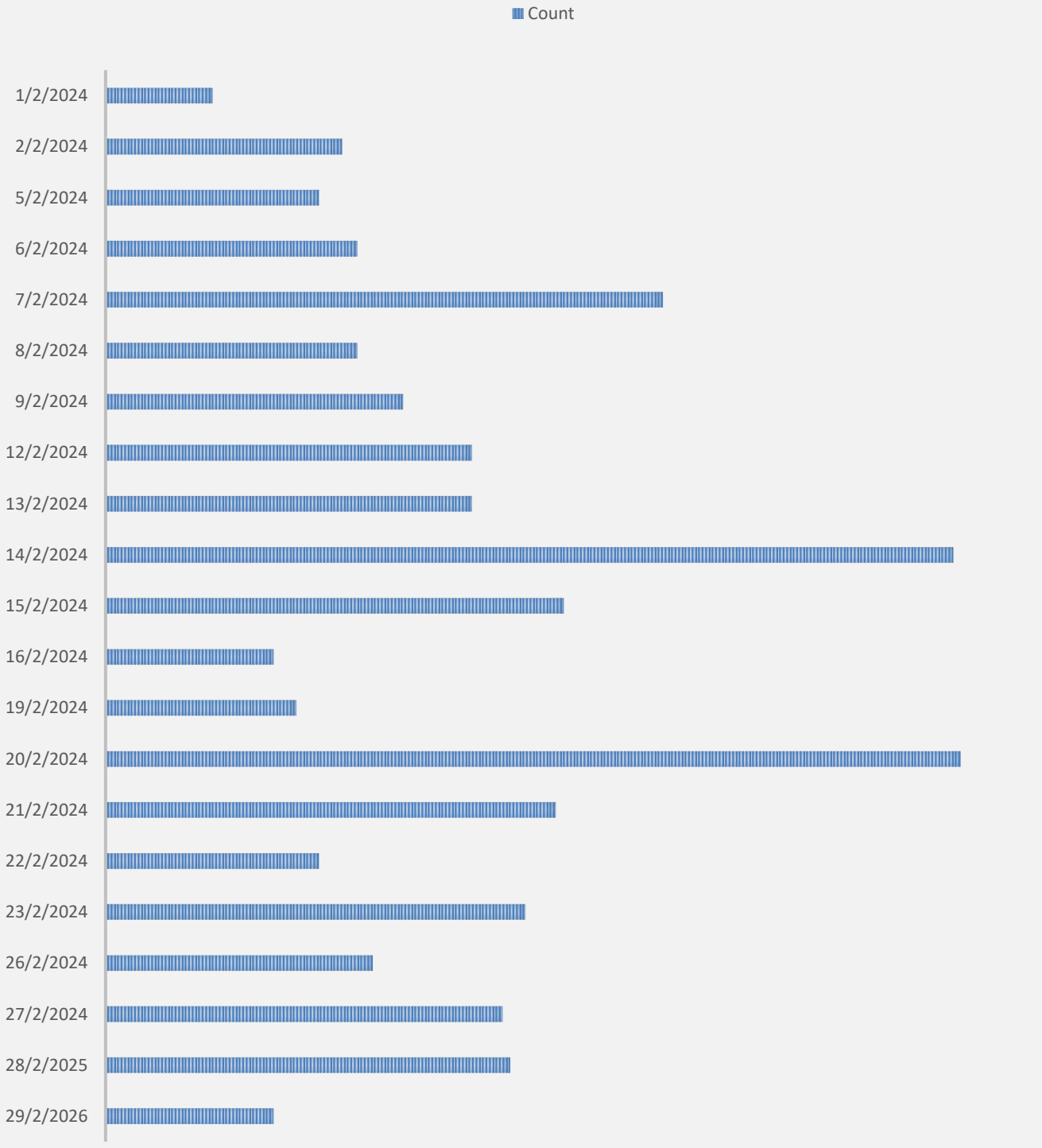
Product-wise Released Non-CVE ID or Zero Day Vulnerabilities Count



Critical CVE Count

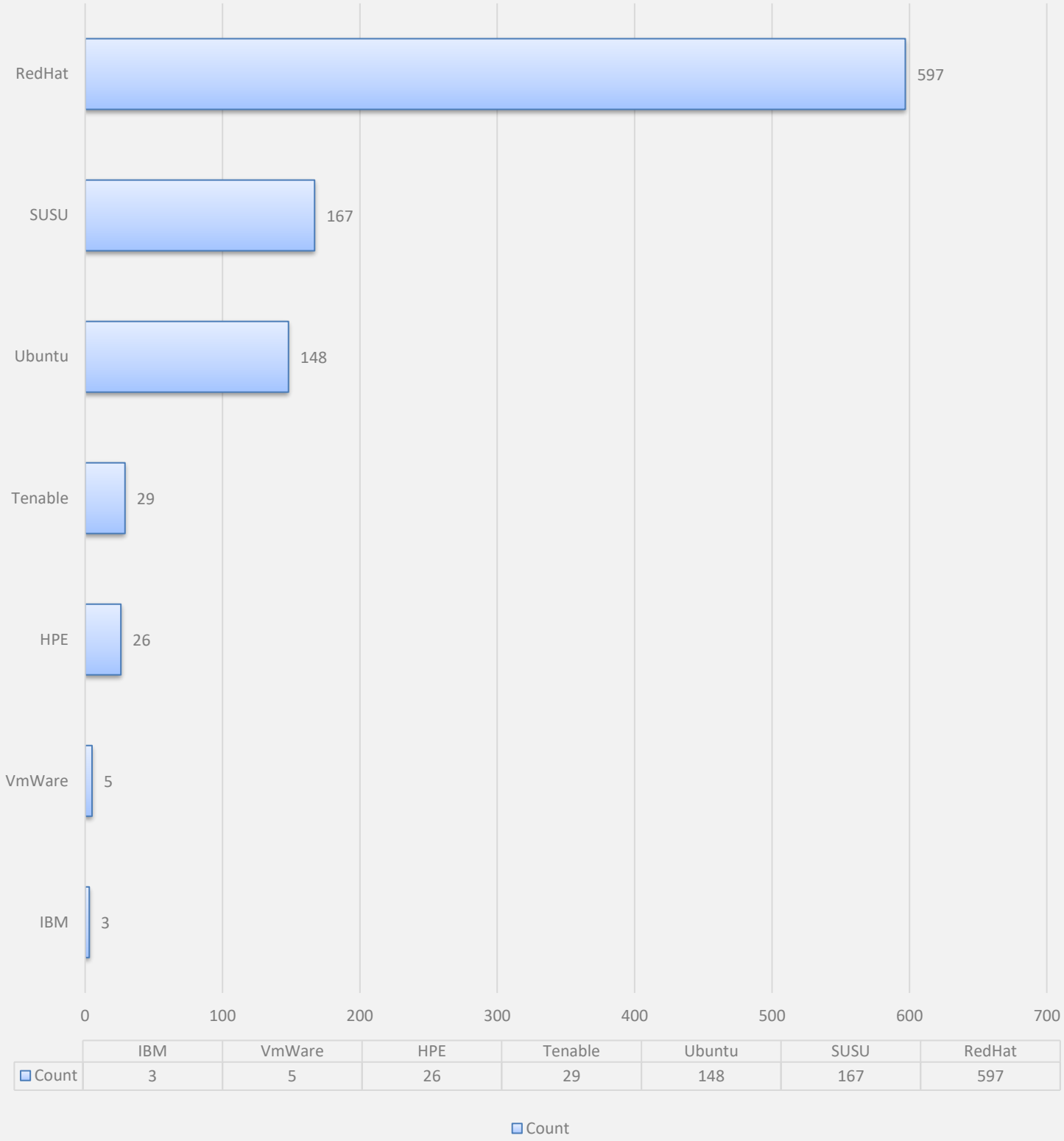


Date-wise Released Vulnerabilities Count, Fortnightly Summarized



	29/2/2026	28/2/2025	27/2/2024	26/2/2024	23/2/2024	22/2/2024	21/2/2024	20/2/2024	19/2/2024	16/2/2024	15/2/2024	14/2/2024	13/2/2024	12/2/2024	9/2/024	28/2/024	27/2/024	26/2/024	25/2/024	22/2/024	21/2/024
Count	22	53	52	35	55	28	59	112	25	22	60	111	48	48	39	33	73	33	28	31	14

Product-wise Chart for CVE



	IBM	VmWare	HPE	Tenable	Ubuntu	SUSU	RedHat
Count	3	5	26	29	148	167	597

TOP VULNERABILITIES OF THE MONTH

DATE	CVE ID	Vendor	Summary	Recommendation
05-02-24	CVE-2023-39325 CVE-2023-45142 CVE-2023-47108 CVE-2023-49568 CVE-2023-49569	RedHat	OpenShift Container Platform 4.14.11 bug fix and security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:0642
06-02-24	CVE-2023-2976 CVE-2020-8908 CVE-2023-46589 CVE-2023-20863 CVE-2016-3088 CVE-2023-46604 CVE-2020-27853 CVE-2021-41093 CVE-2017-7657 CVE-2017-7658 CVE-2023-44981 CVE-2023-20862 CVE-2023-20861 CVE-2022-42004 CVE-2022-42003 CVE-2022-25883 CVE-2023-28155	HPE	HPE Unified OSS Console Assurance Monitoring (UOCAM), Multiple Vulnerabilities	Updates are available please see below reference link: https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04590en_us
08-02-24	CVE-2023-49568 CVE-2023-49569	RedHat	Red Hat Advanced Cluster Management 2.7.11 security and bug fix container update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:0729
15-02-24	CVE-2023-36665	IBM	QRadar Suite Software includes components with multiple known vulnerabilities	Updates are available please see below reference link: https://www.ibm.com/support/pages/node/7118351
22-02-24	CVE-2024-22245 CVE-2024-22250	VMWare	Addressing Arbitrary Authentication Relay and Session Hijack Vulnerabilities in Deprecated VMware Enhanced Authentication Plug-in	Updates are available please see below reference link: https://www.vmware.com/security/advisories/VMSA-2024-0003.html
23-02-24	CVE-2024-0057 CVE-2024-20672	Tenable	Tenable Identity Exposure Version 3.59.4 Fixes Multiple Vulnerabilities	Updates are available please see below reference link: https://www.tenable.com/security/tns-2024-04
28-02-24	CVE-2021-35937 CVE-2021-35938 CVE-2021-35939 CVE-2023-3978 CVE-2023-5363 CVE-2023-5981 CVE-2023-27043 CVE-2023-39325 CVE-2023-39326 CVE-2023-45142	Redhat	OpenShift Container Platform 4.15.0 security and extras update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2023:7197

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**