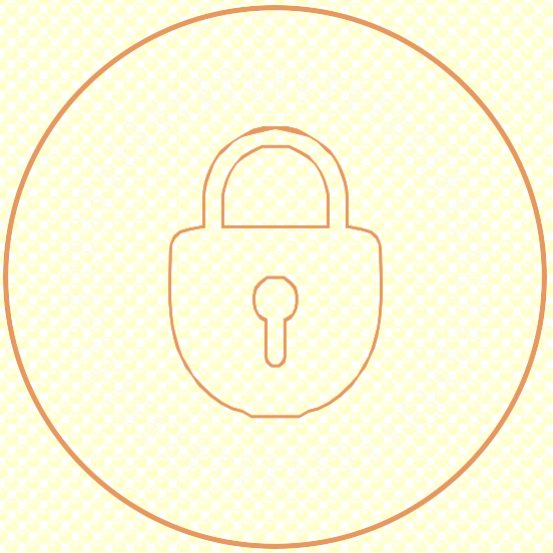
SECURITY INTELLIGENCE ADVISORY



01st May 2024 – 31st May 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.

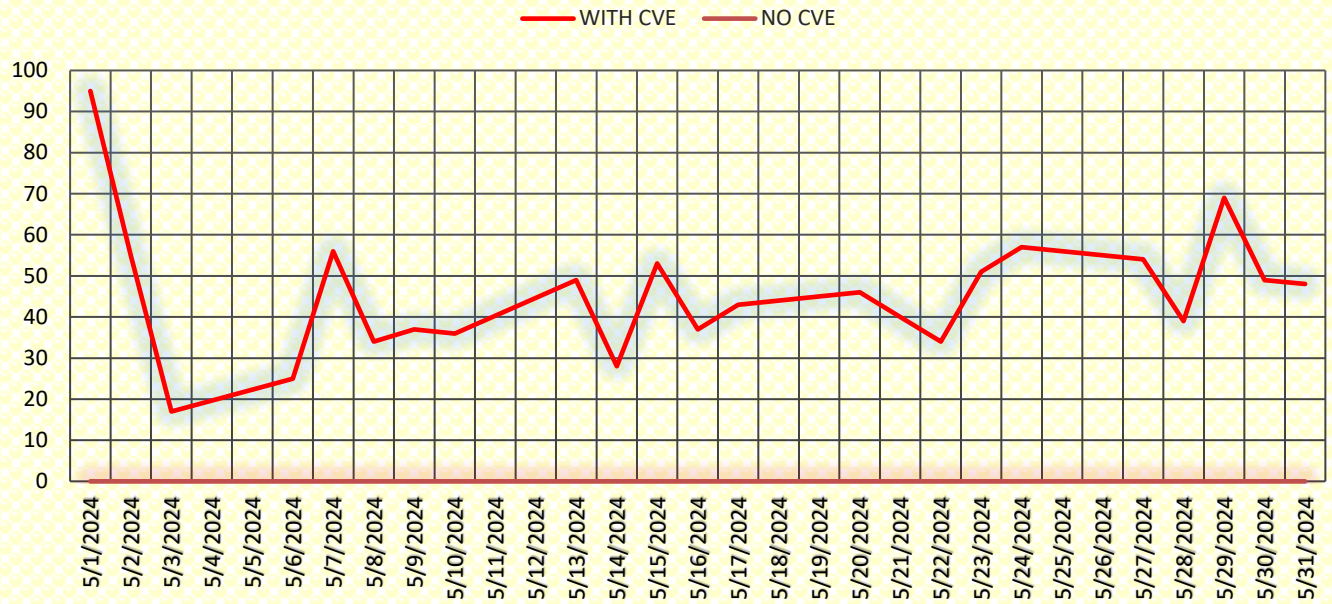
One effective way to stay on top of these vulnerabilities is by conducting regular vulnerability assessments. These periodic assessments cover your entire IT infrastructure and help you identify new threats that may have emerged. This proactive practice enables you to stay abreast of the current state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

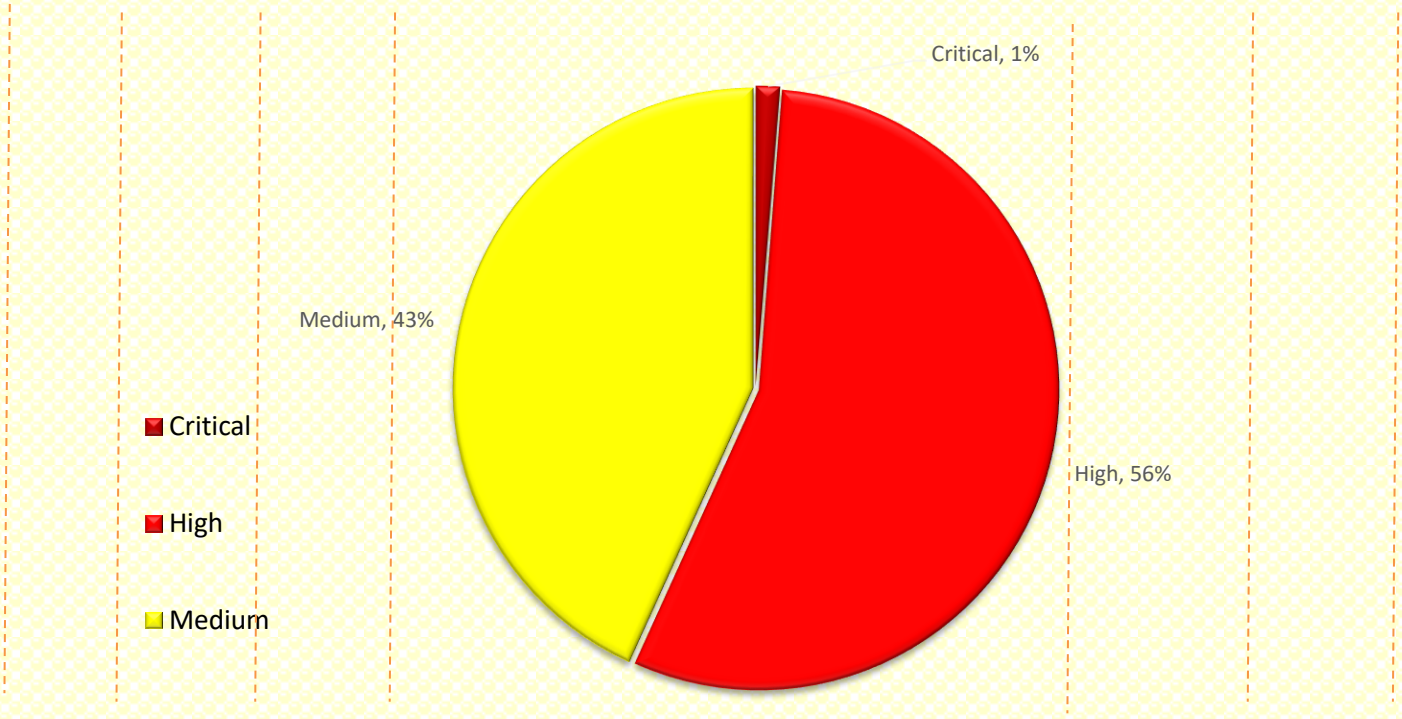
EXECUTIVE SUMMARY

Overall Monthly Vulnerability Trend Chart



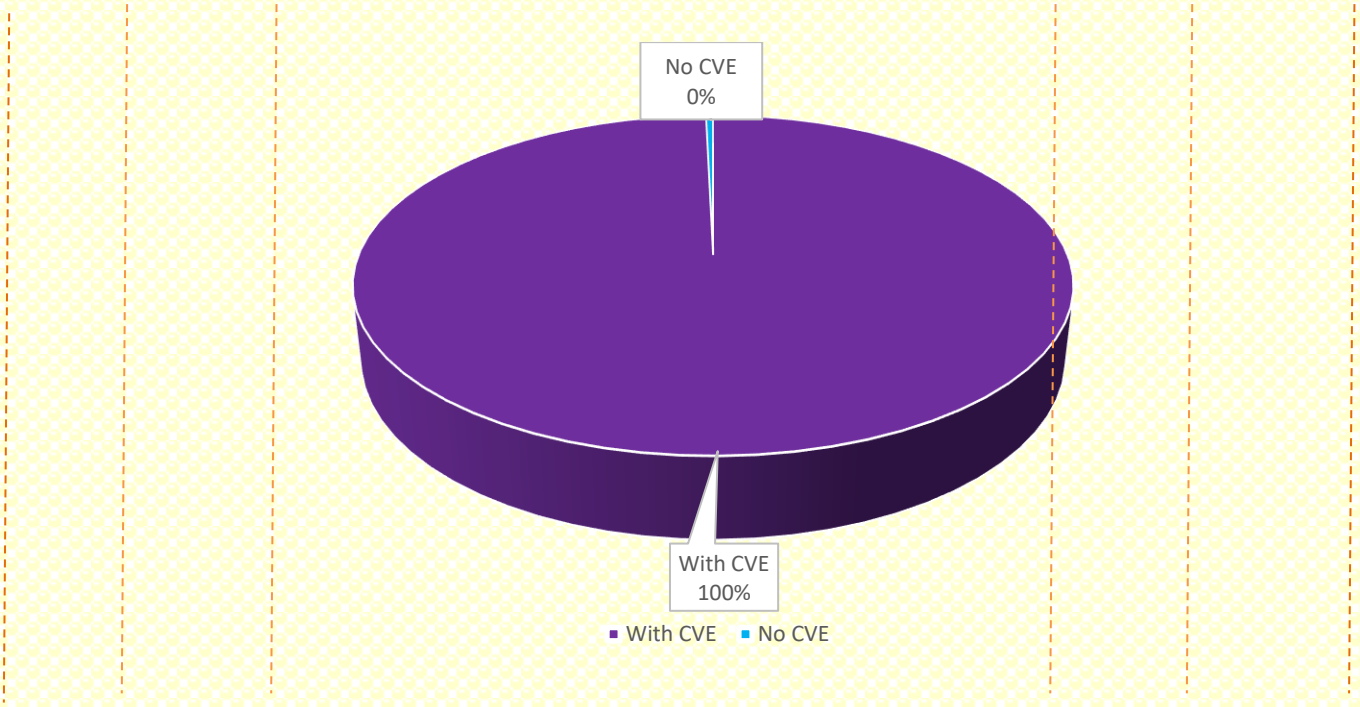
Released Vulnerabilities and Severity Count:

This graph presents threat levels based on vulnerability identified.

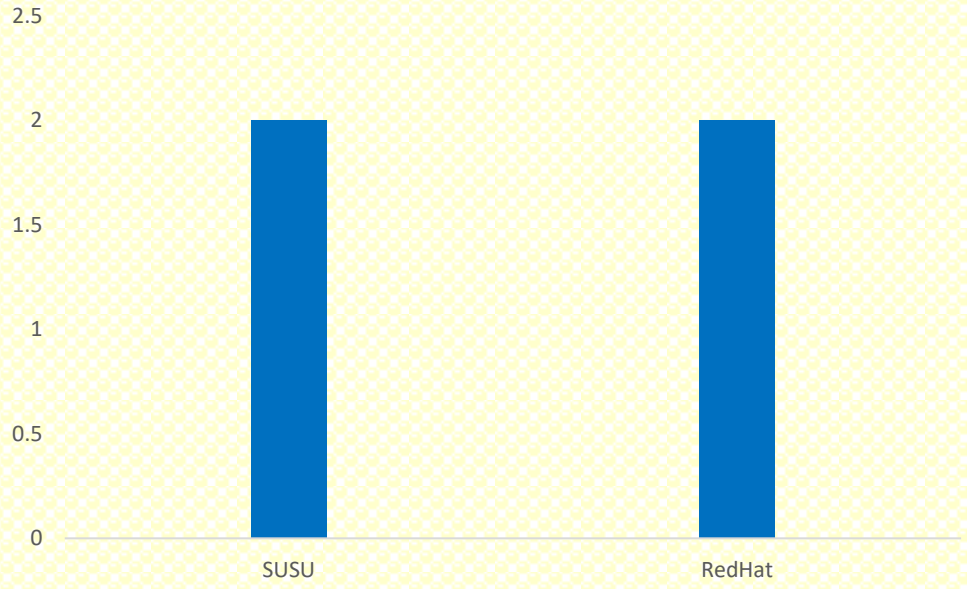


EXECUTIVE SUMMARY

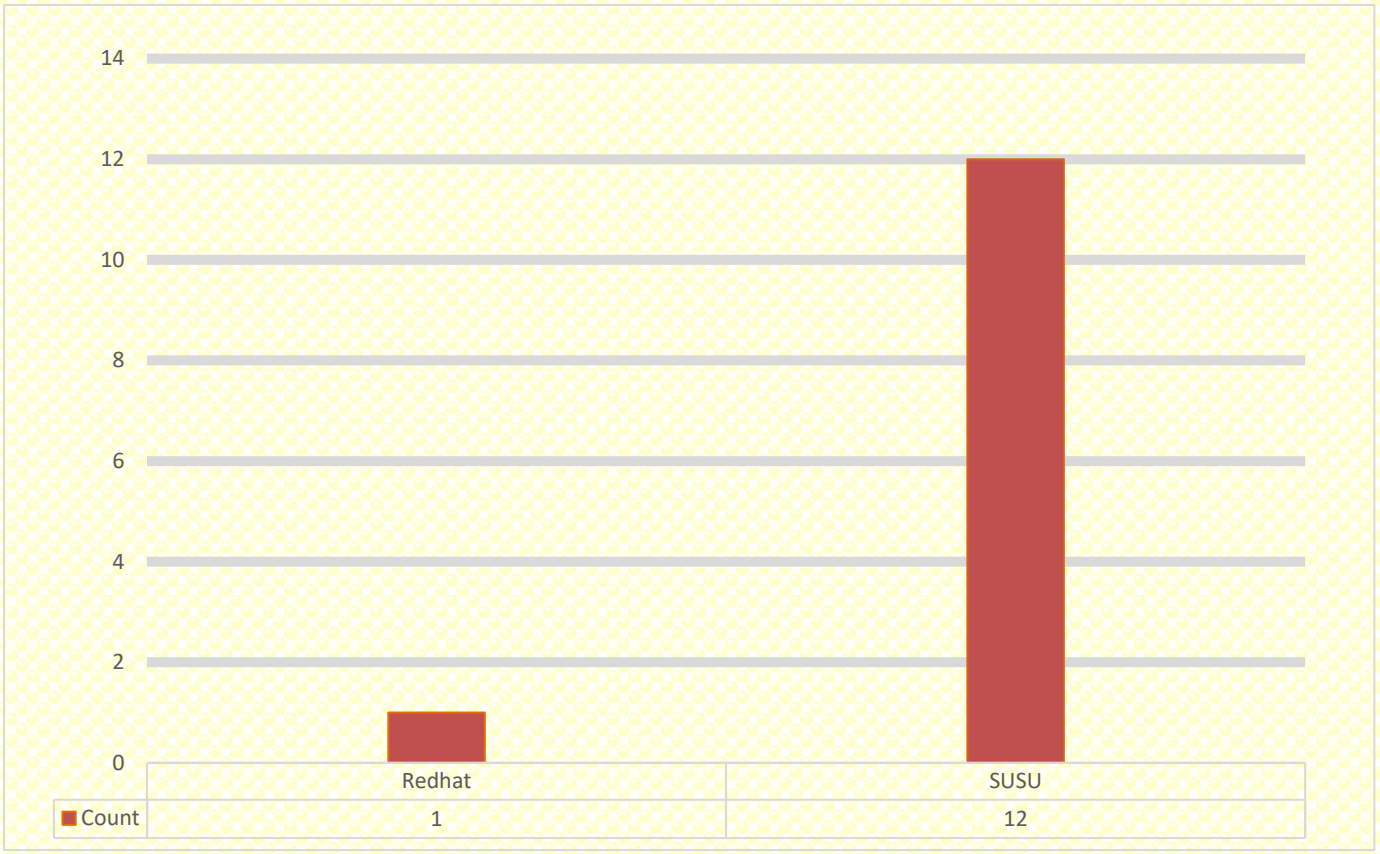
This graph presents the total vulnerabilities released, including zero-day vulnerability with their count.



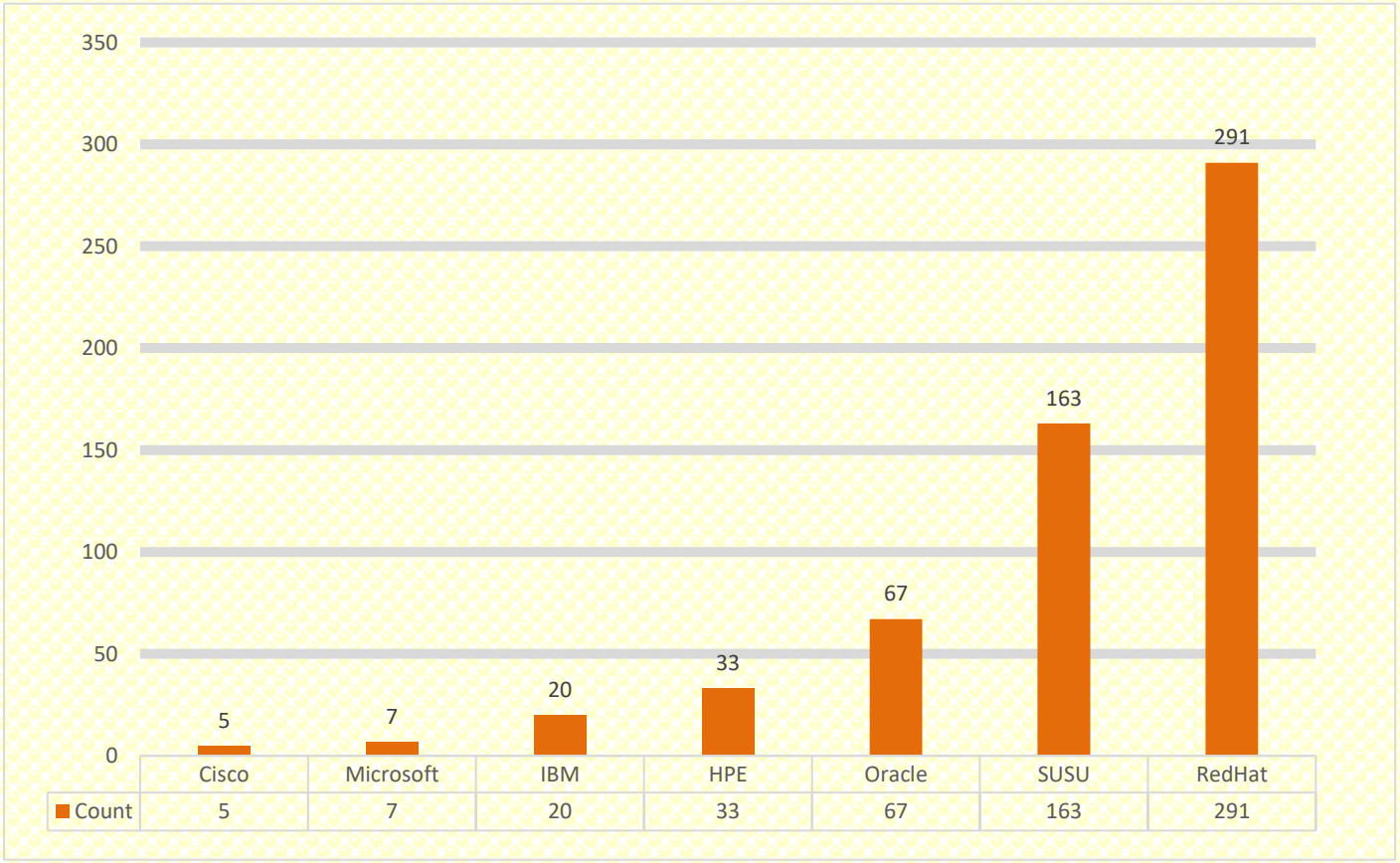
Product-wise Released Non-CVE ID or Zero Day Vulnerabilities Count



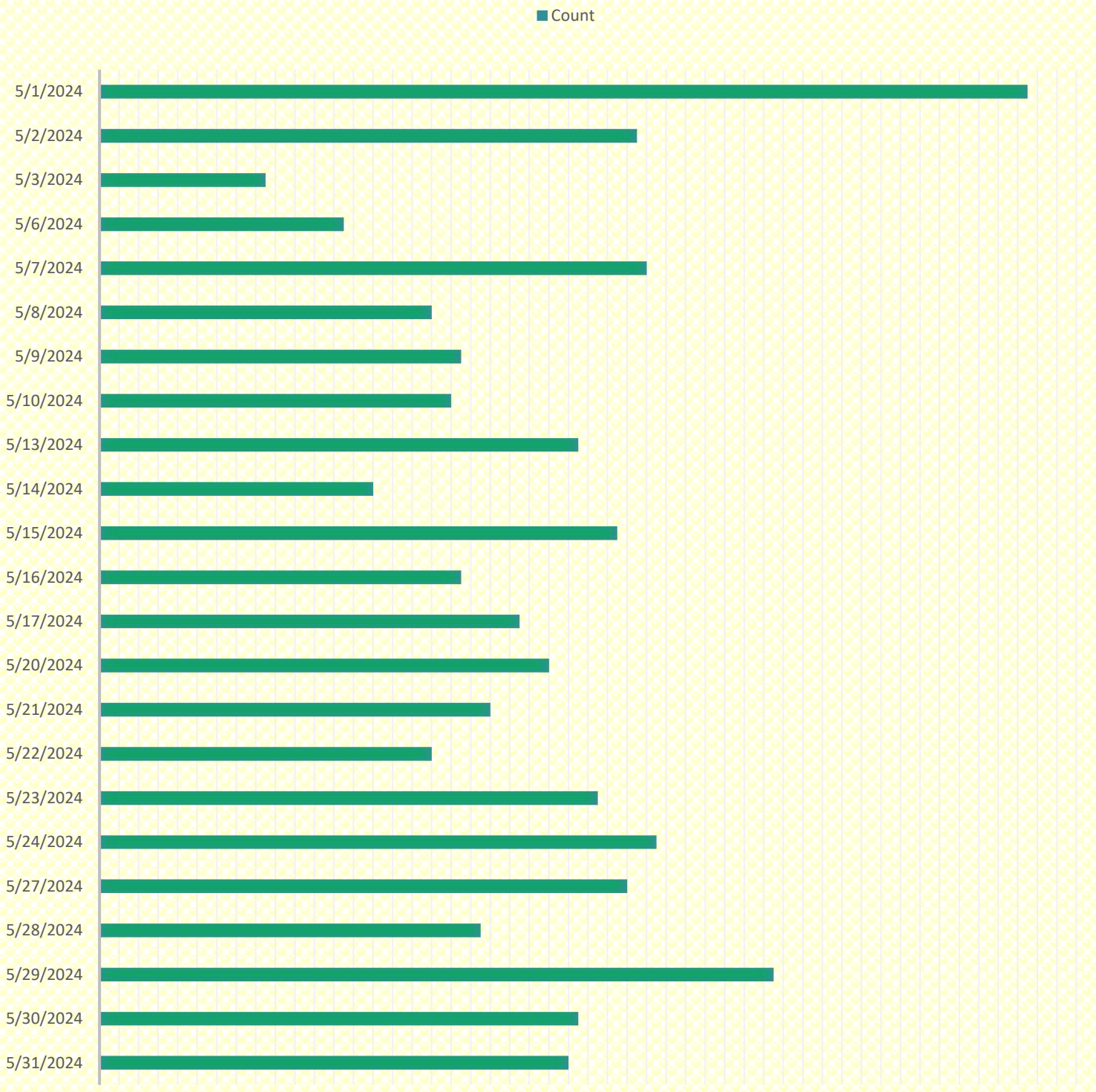
Critical CVE Count: -



HIGH CVE Count: -

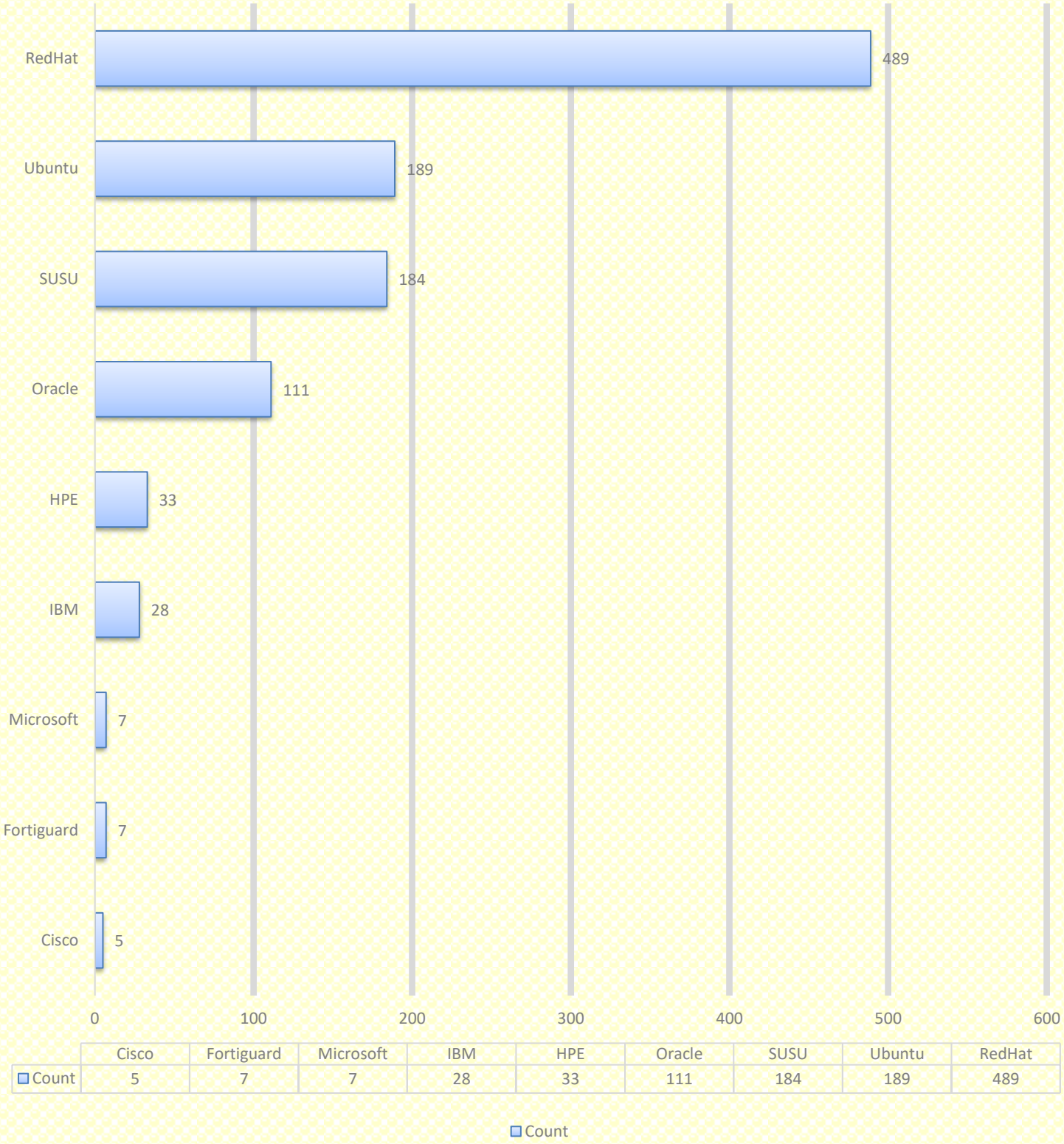


Date-wise Released Vulnerabilities Count, Fortnightly Summarized



	5/31/2024	5/30/2024	5/29/2024	5/28/2024	5/27/2024	5/24/2024	5/23/2024	5/22/2024	5/21/2024	5/20/2024	5/17/2024	5/16/2024	5/15/2024	5/14/2024	5/13/2024	5/10/2024	5/9/2024	5/8/2024	5/7/2024	5/6/2024	5/3/2024	5/2/2024	5/1/2024
Count	48	49	69	39	54	57	51	34	40	46	43	37	53	28	49	36	37	34	56	25	17	55	95

Product-wise Chart for CVE



	Cisco	Fortiguard	Microsoft	IBM	HPE	Oracle	SUSU	Ubuntu	RedHat
Count	5	7	7	28	33	111	184	189	489

SOME VULNERABILITITIES OF THE MONTH

SL.NO	CVE ID	Vendor	Summary	Recommendation
01	CVE-2020-35654 CVE-2021-23437 CVE-2021-25289 CVE-2021-25290 CVE-2021-25292 CVE-2021-25293 CVE-2021-27921 CVE-2021-27922 CVE-2021-27923 CVE-2021-34552 CVE-2022-22815 CVE-2022-22816	SUSU	Security update for python-Pillow	Updates are available please see below reference link: https://www.suse.com/support/update/announcement/2024/suse-su-20241673-1/
02	CVE-2023-49569	RedHat	Red Hat Ceph Storage 6.1 security and bug fix update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:2631
03	CVE-2014-1745 CVE-2023-41983 CVE-2023-39928 CVE-2024-23213 CVE-2024-23206 CVE-2023-40414 CVE-2023-32359 CVE-2023-42890 CVE-2023-42883 CVE-2023-42852	Oracle	webkit2gtk3 security update	Updates are available please see below reference link: https://linux.oracle.com/errata/ELSA-2024-2126.html
04	CVE-2023-45288 CVE-2024-1753 CVE-2024-28180	RedHat	OpenShift Container Platform 4.13.41 packages and security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:2049
05	CVE-2024-31080 CVE-2024-31081 CVE-2024-31083	Oracle	tigervnc security update	Updates are available please see below reference link: https://linux.oracle.com/errata/ELSA-2024-2616.html
06	CVE-2017-18214 CVE-2022-24785 CVE-2016-4055 CVE-2022-31129	IBM	Multiple vulnerabilities in moment.js affect IBM Storage Scale	Updates are available please see below reference link: https://www.ibm.com/support/pages/node/7150528
07	CVE-2023-1973 CVE-2023-4639 CVE-2024-1459	RedHat	Red Hat JBoss Enterprise Application Platform 8.0 security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:2763
08	CVE-2023-51775 CVE-2024-22329 CVE-2024-22354 CVE-2023-50312 CVE-2024-27270	IBM	Due to the use of IBM Websphere Application Server Liberty, IBM TXSeries for Multiplatforms is vulnerable to Denial of Service, Weaker than exected security, Cross-site scripting and Server-side request forgery (SSRF).	Updates are available please see below reference link: https://www.ibm.com/support/pages/node/7150669

09	CVE-2024-30156	RedHat	varnish security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:2820
10	CVE-2024-32002	Microsoft	Recursive clones on case-insensitive filesystems that support symlinks are susceptible to Remote Code	Updates are available please see below reference link: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-32002
11	CVE-2024-29996	Microsoft	Windows Common Log File System Driver Elevation of Privilege Vulnerability	Updates are available please see below reference link: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-29996
12	CVE-2024-30006	Microsoft	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	Updates are available please see below reference link: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30006
13	CVE-2021-30639 CVE-2021-30640 CVE-2021-33037 CVE-2021-41079 CVE-2021-42340 CVE-2021-43980 CVE-2022-23181 CVE-2022-29885 CVE-2022-34305 CVE-2022-42252 CVE-2022-45143 CVE-2023-24998 CVE-2023-28709 CVE-2023-28708 CVE-2023-34981 CVE-2023-41080 CVE-2023-42794 CVE-2023-42795 CVE-2023-44487 CVE-2023-45648 CVE-2023-46589 CVE-2024-23672 CVE-2024-24549	HPE	HP-UX 11i v3 Tomcat-based Servlet Engine, Multiple Vulnerabilities	Updates are available please see below reference link: https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbux04652en_us&docLocale=en_US
14	CVE-2024-3651 CVE-2024-0450 CVE-2023-6597	Oracle	python39:3.9 and python39-devel:3.9 security update	Updates are available please see below reference link: https://linux.oracle.com/errata/ELSA-2024-3466.html
15	CVE-2023-4408 CVE-2023-50387 CVE-2023-50868	Redhat	bind and dhcp security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:3271
16	CVE-2024-27983 CVE-2024-28182 CVE-2024-25629 CVE-2024-27982 CVE-2024-22025	Oracle	nodejs:18 security update	Updates are available please see below reference link: https://linux.oracle.com/errata/ELSA-2024-2780.html
17	CVE-2024-4367 CVE-2024-4767 CVE-2024-4768 CVE-2024-4769 CVE-2024-4770 CVE-2024-4777	Redhat	firefox security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:2882

SOME ZERO-DAY VULNERABILITITIES OF THE MONTH

SL.NO	Title	Vendor	Severity	Summary
01	security update Logging for Red Hat OpenShift - 5.9.1	Redhat	Medium	Logging Subsystem for Red Hat OpenShift for ARM 64 5 for RHEL 9 aarch64 Logging Subsystem for Red Hat OpenShift 5 for RHEL 9 x86_64 Logging Subsystem for Red Hat OpenShift for IBM Power, little endian 5 for RHEL 9 ppc64le Logging Subsystem for Red Hat OpenShift for IBM Z and LinuxONE 5 for RHEL 9 s390x
02	Security update for skopeo	Susu	High	Basesystem Module 15-SP5 openSUSE Leap 15.3 openSUSE Leap 15.5 SUSE Enterprise Storage 7.1 SUSE Linux Enterprise Desktop 15 SP4 LTSS 15-SP4 SUSE Linux Enterprise Desktop 15 SP5 SUSE Linux Enterprise High Performance Computing 15 SP3 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise High Performance Computing 15 SP5
03	RedHat Build of Apache Camel 4.0 for Quarkus 3.2	Redhat	High	An update for Red Hat Build of Apache Camel 4.0 for Quarkus 3.2 update is now available (RHBQ 3.2.12.GA). The purpose of this text-only errata is to inform you about the enhancements that improve your developer experience and ensure the security and stability of your products.
04	Security update for the Linux Kernel	Susu	High	The SUSE Linux Enterprise 15 SP5 kernel was updated to receive various security bugfixes. This update fixes a regression with kerberized nfs4 shares in the previous update

Global Presence

USA / Sattrix Information Security Incorporation
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**