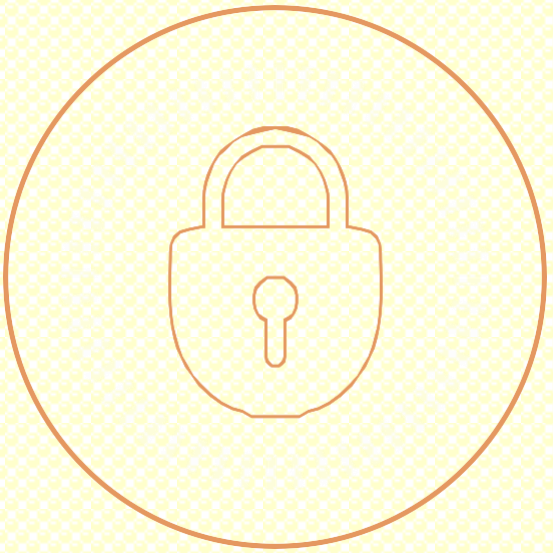
Gattrix™

SECURITY INTELLIGENCE ADVISORY



01st Apr 2024 – 30th Apr 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.

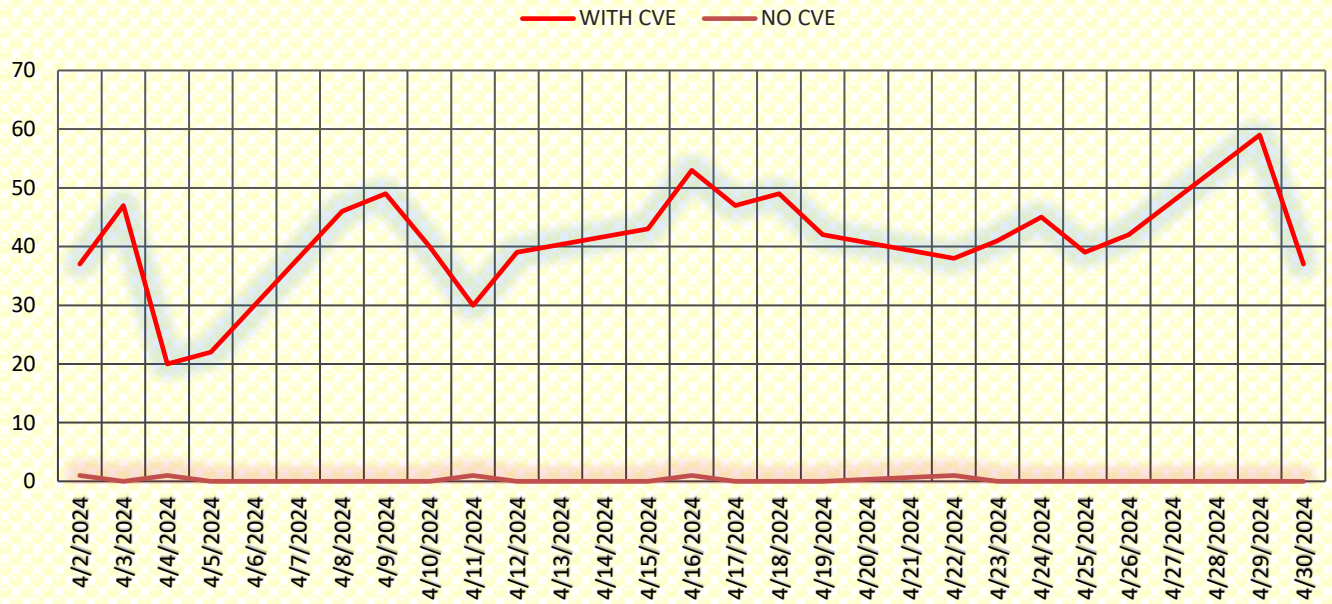
One effective way to stay on top of these vulnerabilities is by conducting regular vulnerability assessments. These periodic assessments cover your entire IT infrastructure and help you identify new threats that may have emerged. This proactive practice enables you to stay abreast of the current state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

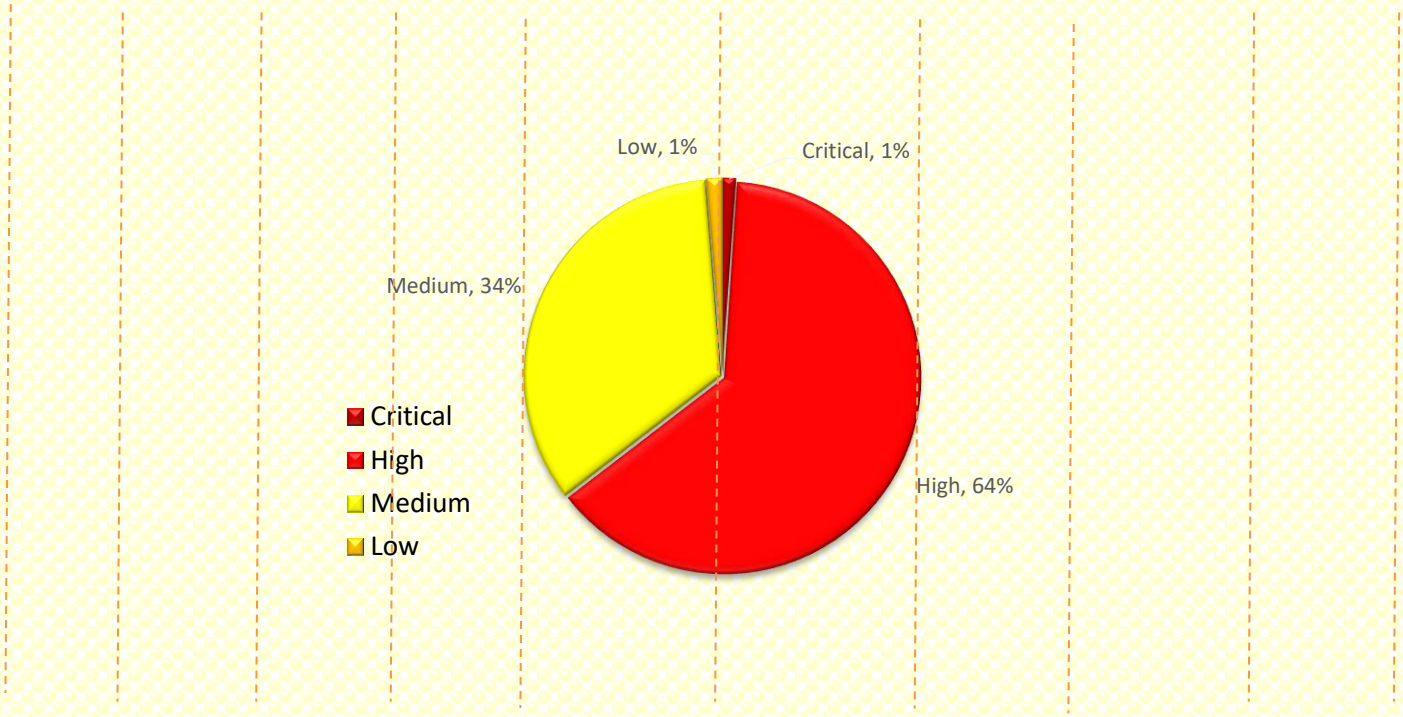
EXECUTIVE SUMMARY

Overall Monthly Vulnerability Trend Chart



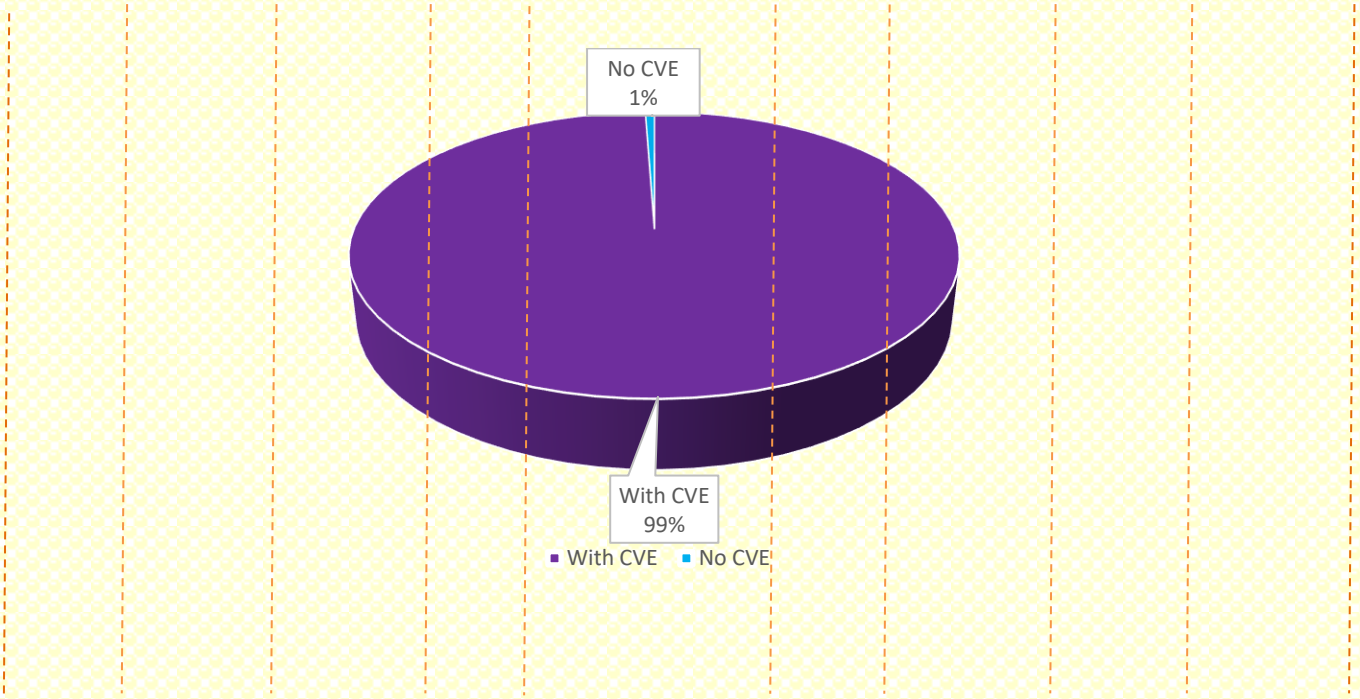
Released Vulnerabilities and Severity Count:

This graph presents threat levels based on vulnerability identified.

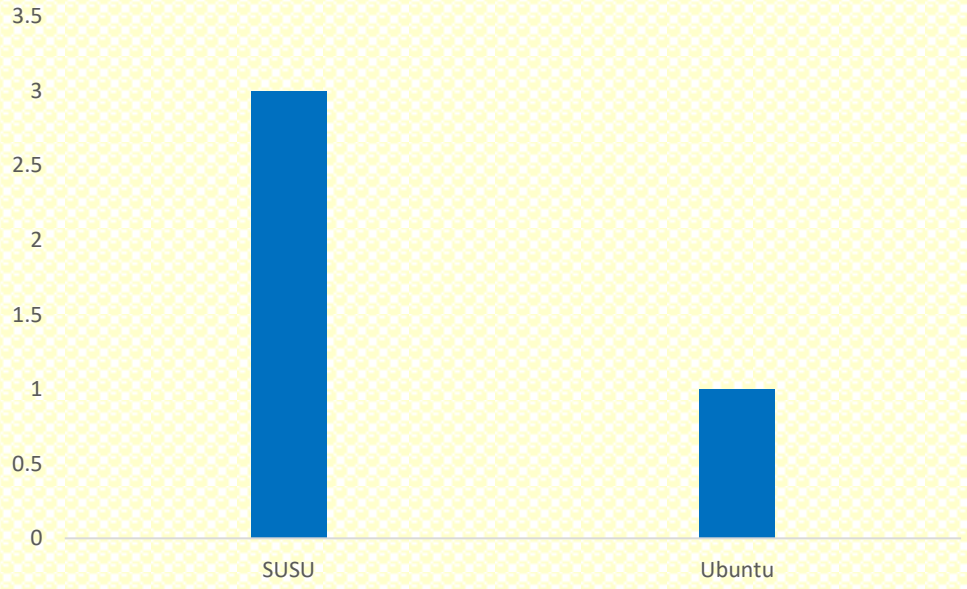


EXECUTIVE SUMMARY

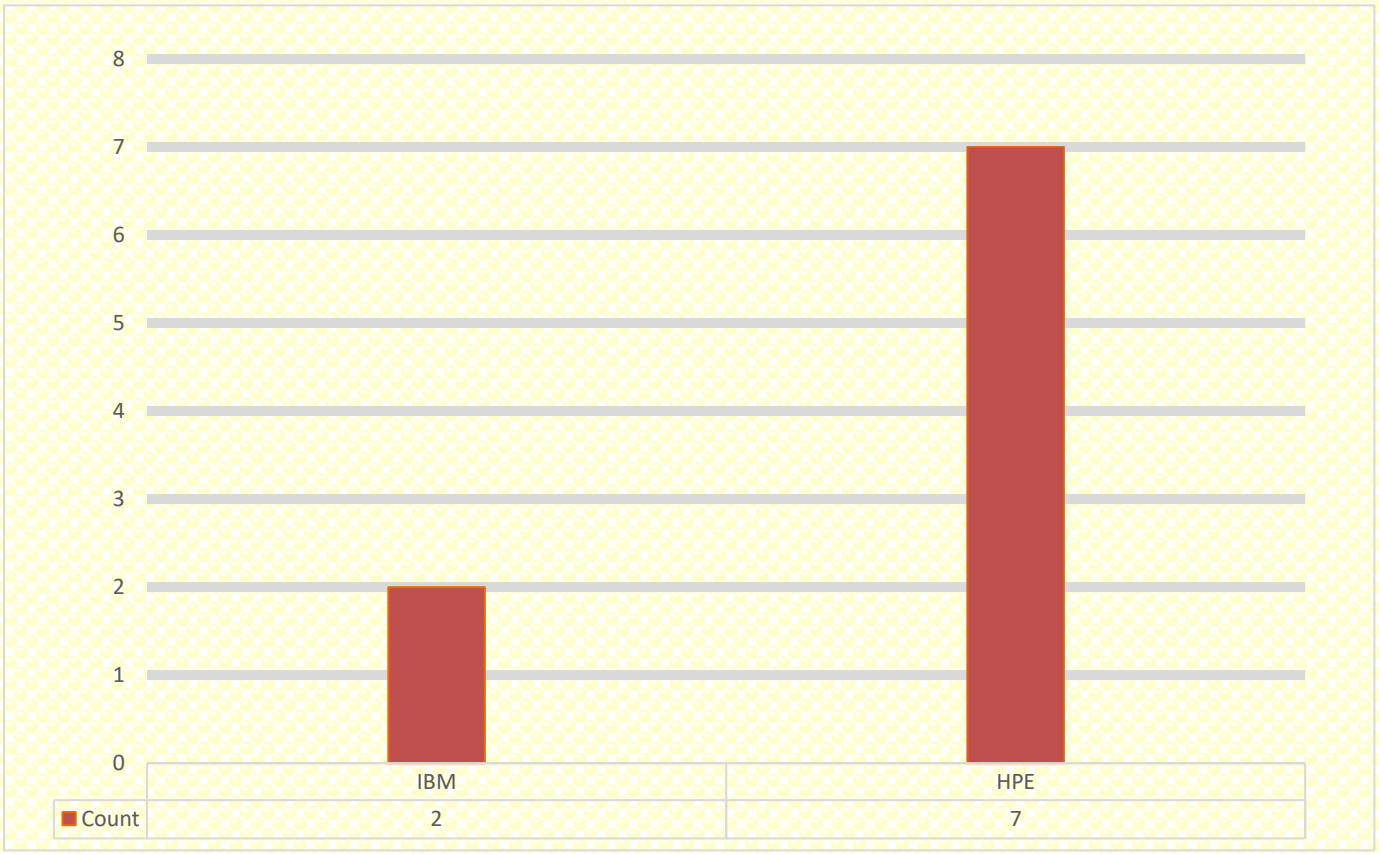
This graph presents the total vulnerabilities released, including zero-day vulnerability with their count.



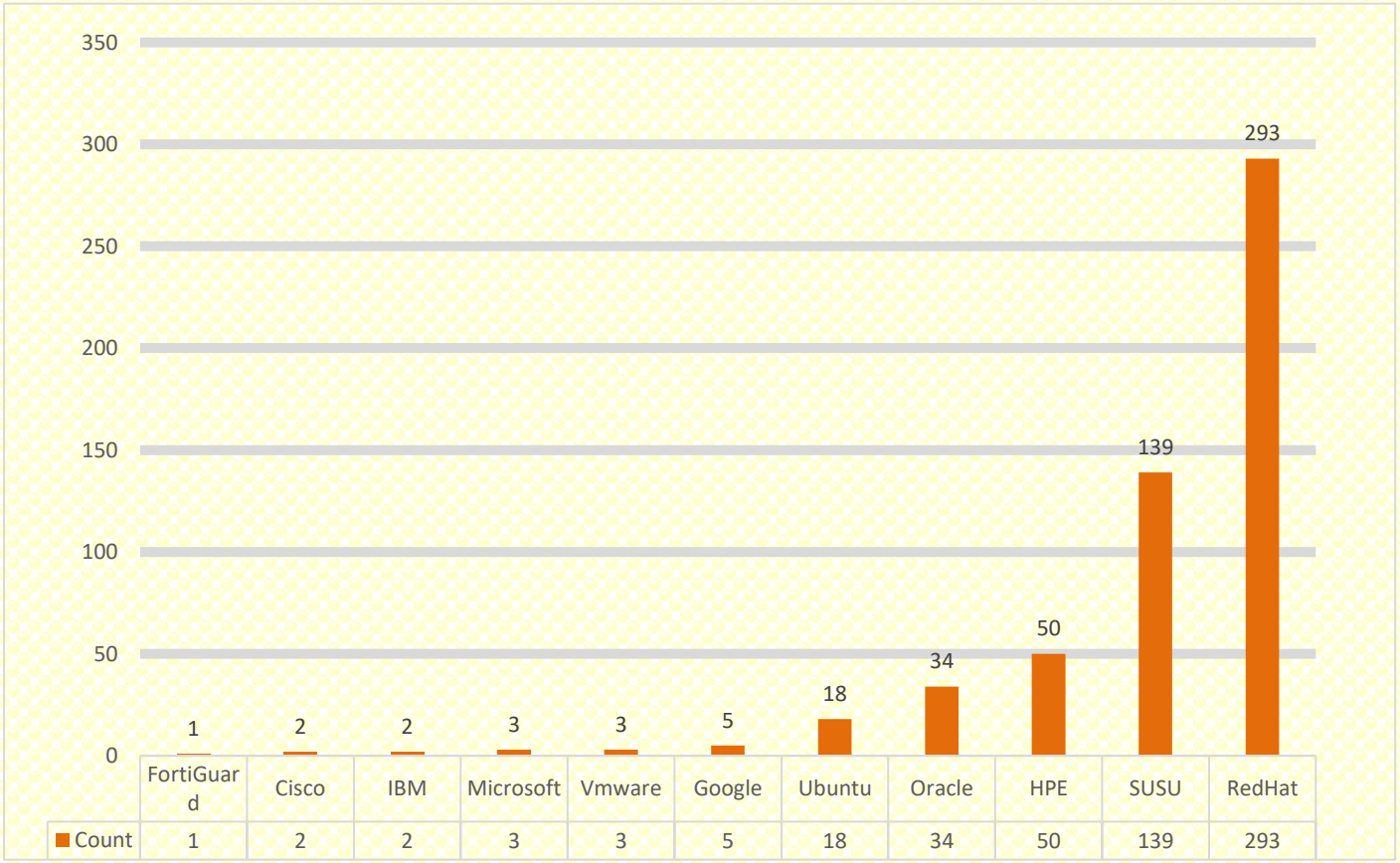
Product-wise Released Non-CVE ID or Zero Day Vulnerabilities Count



Critical CVE Count: -



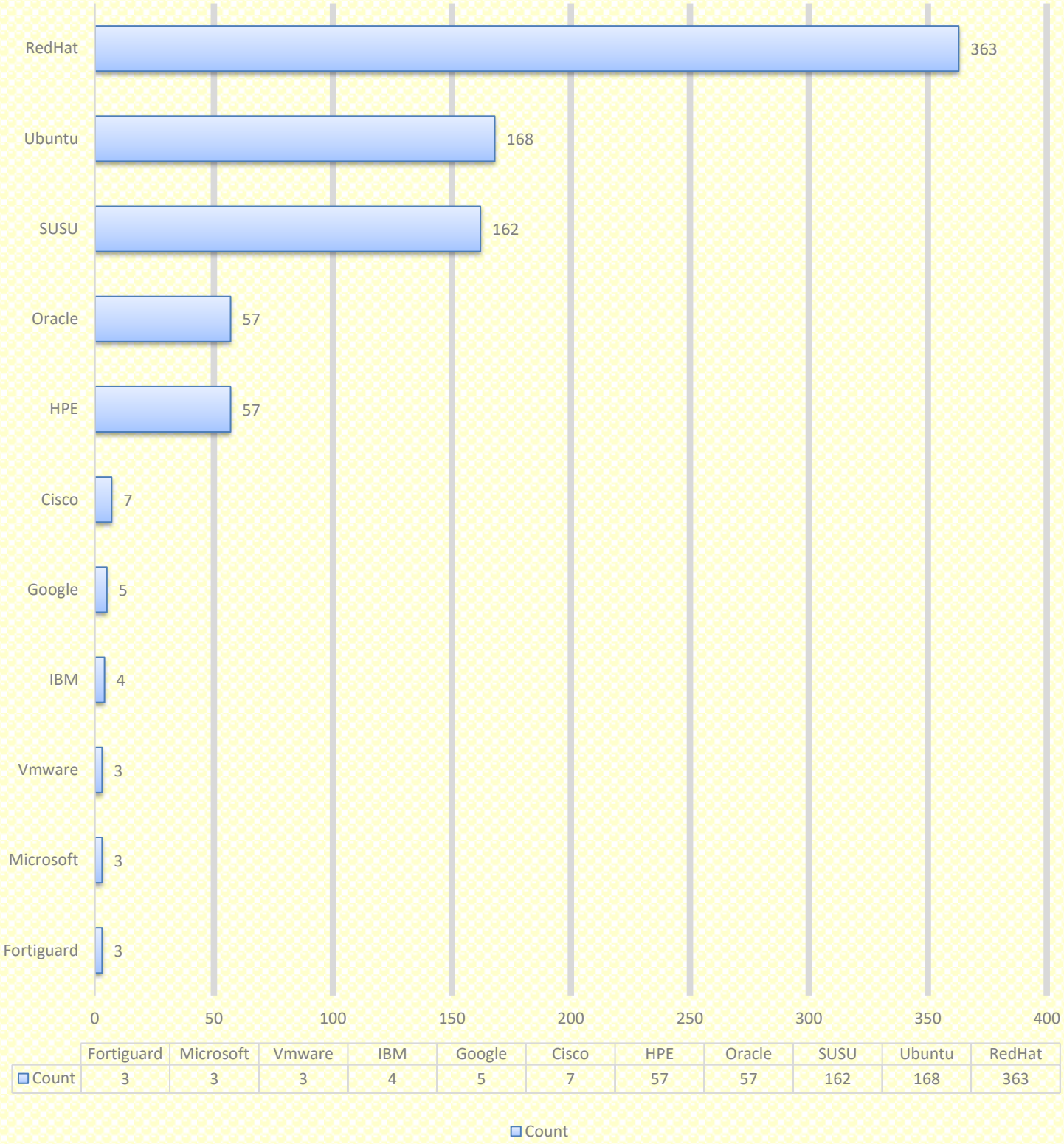
HIGH CVE Count: -



Date-wise Released Vulnerabilities Count, Fortnightly Summarized

	4/30/2024	4/29/2024	4/26/2024	4/25/2024	4/24/2024	4/23/2024	4/22/2024	4/19/2024	4/18/2024	4/17/2024	4/16/2024	4/15/2024	4/12/2024	4/11/2024	4/10/2024	4/9/2024	4/8/2024	4/5/2024	4/4/2024	4/3/2024	4/2/2024
Count	37	59	42	39	45	41	38	42	49	47	53	43	39	30	40	49	46	22	20	47	37

Product-wise Chart for CVE



	Fortiguard	Microsoft	Vmware	IBM	Google	Cisco	HPE	Oracle	SUSU	Ubuntu	RedHat
Count	3	3	3	4	5	7	57	57	162	168	363

SOME VULNERABILITITIES OF THE MONTH

SL.NO	CVE ID	Vendor	Summary	Recommendation
01	CVE-2021-33631 CVE-2022-38096 CVE-2023-6546 CVE-2023-6931 CVE-2023-51042 CVE-2024-0565 CVE-2024-1086	RedHat	kernel security, bug fix, and enhancement update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:1607
02	CVE-2024-20348 CWE-27	Cisco	Cisco Nexus Dashboard Fabric Controller Plug and Play Arbitrary File Read Vulnerability	Updates are available please see below reference link: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfccsrf-TEmZEfJ9
03	CVE-2024-21409	Microsoft	.NET, .NET Framework, and Visual Studio Remote Code Execution Vulnerability	Updates are available please see below reference link: https://www.cve.org/CVERecord?id=CVE-2024-21409
04	CVE-2024-28176 CVE-2024-27307	IBM	IBM App Connect Enterprise is vulnerable to a denial of service and remote attack due to node.js jose module and jsonata-js JSONata	Updates are available please see below reference link: https://www.ibm.com/support/pages/node/7145701
05	CVE-2023-41677	FortiGuard	Execute unauthorized code or commands	Updates are available please see below reference link: https://www.fortiguard.com/psirt/FG-IR-23-493
06	CVE-2021-38578	HPE	HPE Superdome Flex, Superdome Flex 280 and Compute Scale-up Server 3200 Servers, Privilege Elevation and Arbitrary Code Execution	Updates are available please see below reference link: https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04633en_us&docLocale=en_US
07	CVE-2024-2886 CVE-2024-3157 CVE-024-3159 CVE-2024-2887 CVE-2024-2176	Google	ChromeOS Long-term Support (LTS) release notes	Updates are available please see below reference link: https://chromereleases.googleblog.com/2024/04/long-term-support-channel-update-for.html
08	CVE-2023-3611 CVE-2023-3776 CVE-2023-31436 CVE-2023-4921	Oracle	kernel security update	Updates are available please see below reference link: https://linux.oracle.com/errata/ELSA-2024-1831.html
09	CVE-2024-29953 CVE-2022-25236 CVE-2019-6109 CVE-2023-2975 CVE-2023-0466 CVE-2023-0464	HPE	HPE SAN Switches with Brocade Fabric OS (FOS), Multiple Remote and Local Vulnerabilities	Updates are available please see below reference link: https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbst04635en_us&docLocale=en_US
10	CVE-2023-39325 CVE-2024-1394 CVE-2024-24786 CVE-2024-26602 CVE-2024-28180	RedHat	OpenShift Container Platform 4.14.21 bug fix and security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:1765

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**