

SECURITY INTELLIGENCE ADVISORY

01st Dec 2023 – 31st Dec 2023



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.

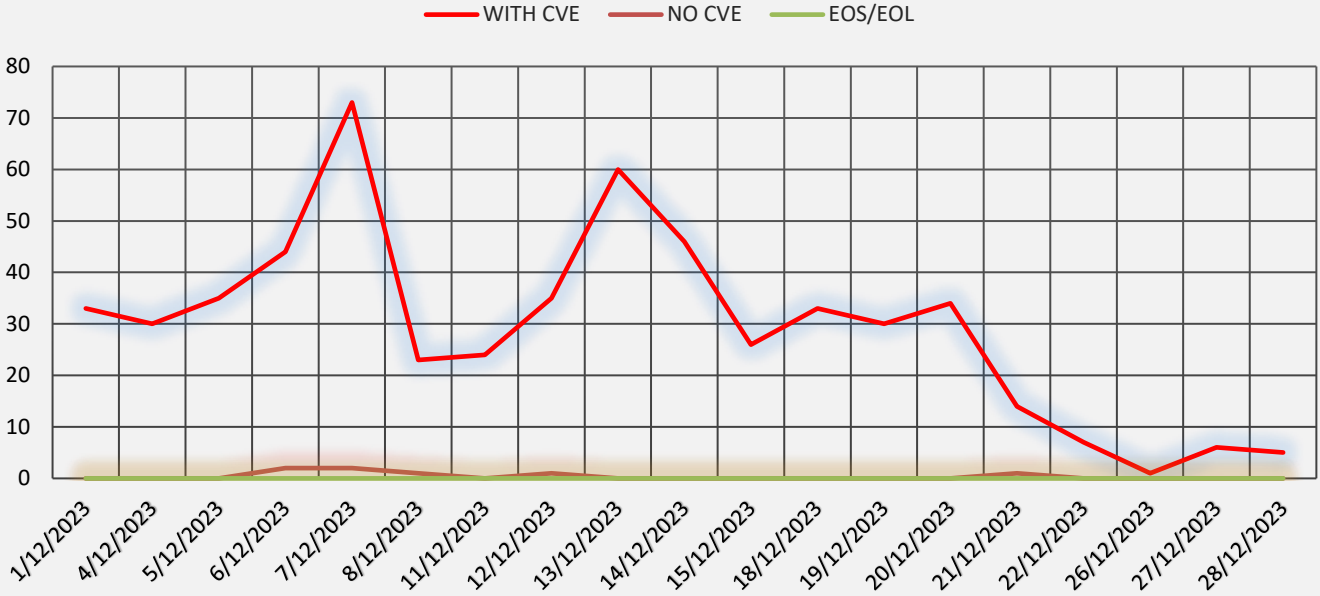
One effective way to stay on top of these vulnerabilities is by conducting regular vulnerability assessments. These periodic assessments cover your entire IT infrastructure and help you identify new threats that may have emerged. This proactive practice enables you to stay abreast of the current state 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 Satrix 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 Satrix 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 Satrix Advisory descriptions include severity, under investigation product, Affected Product, CVE ID, Satrix score, reference links, and remediation recommendations.
 - Satrix researchers complete the vulnerability assessment process within 5 business working days.
-

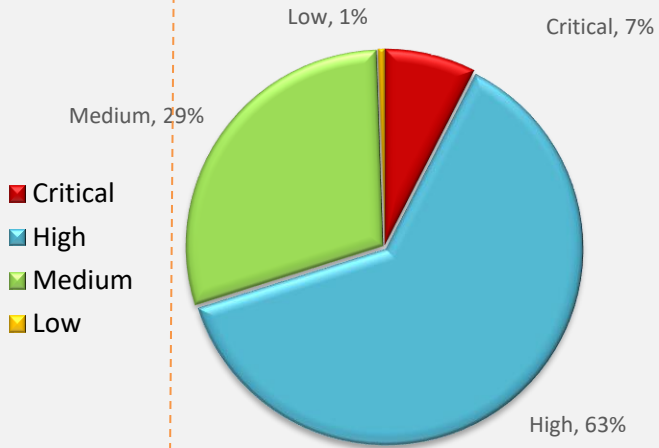
EXECUTIVE SUMMARY

Overall Monthly Vulnerability Trend Chart



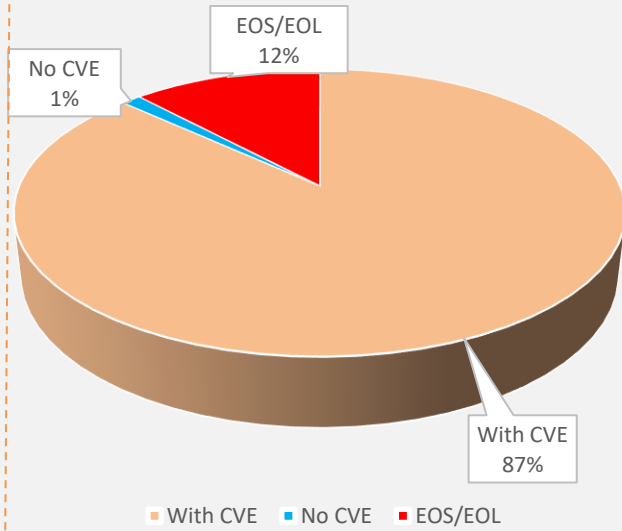
Released Vulnerabilities and Severity Count:

This graph presents threat levels based on vulnerability identified.

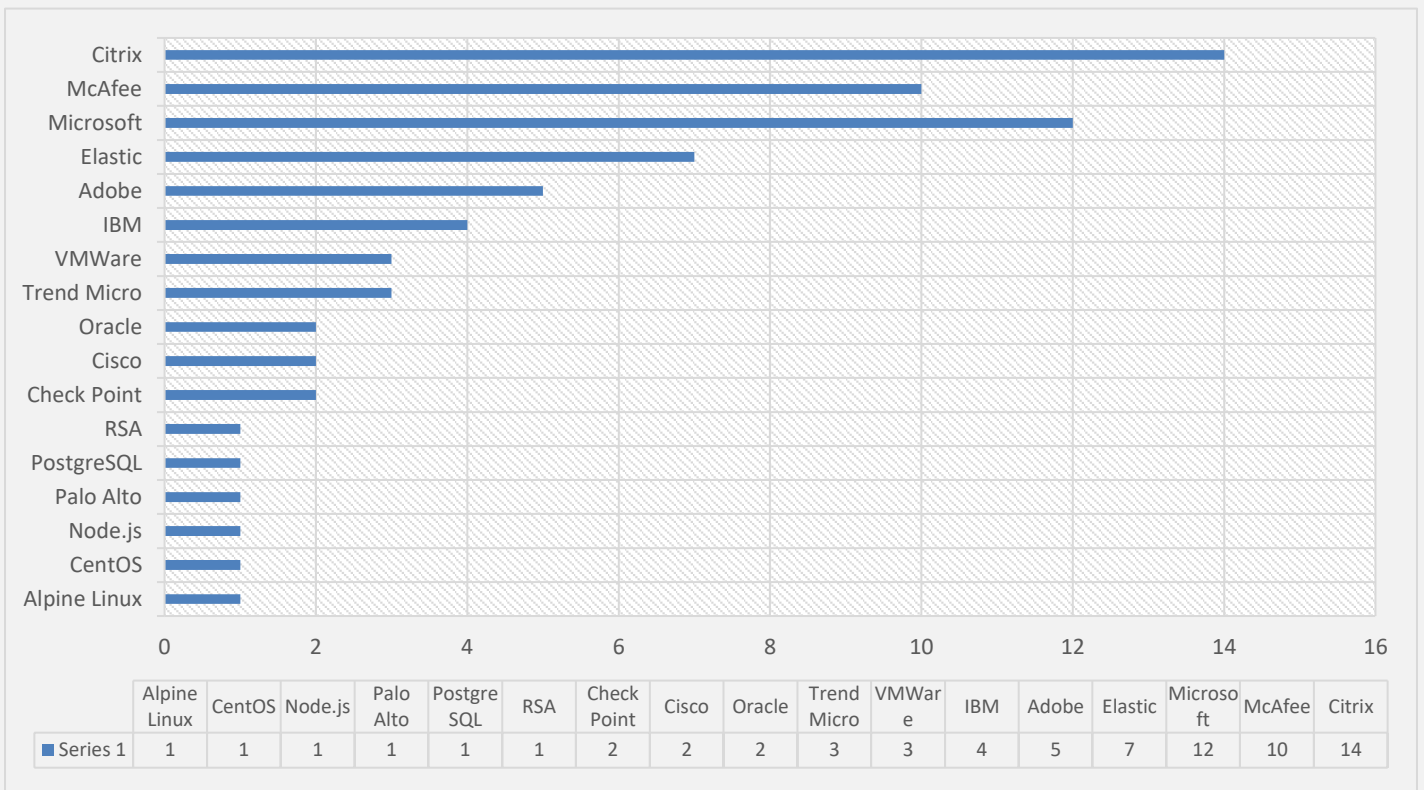


EXECUTIVE SUMMARY

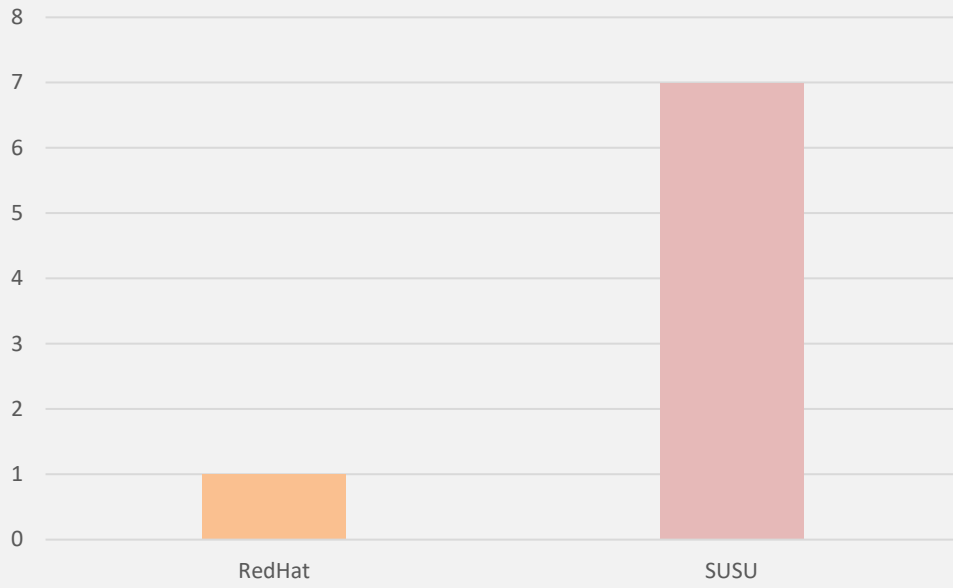
This graph presents the total vulnerabilities released, including zero-day vulnerability and EOS/EOL, with their count.



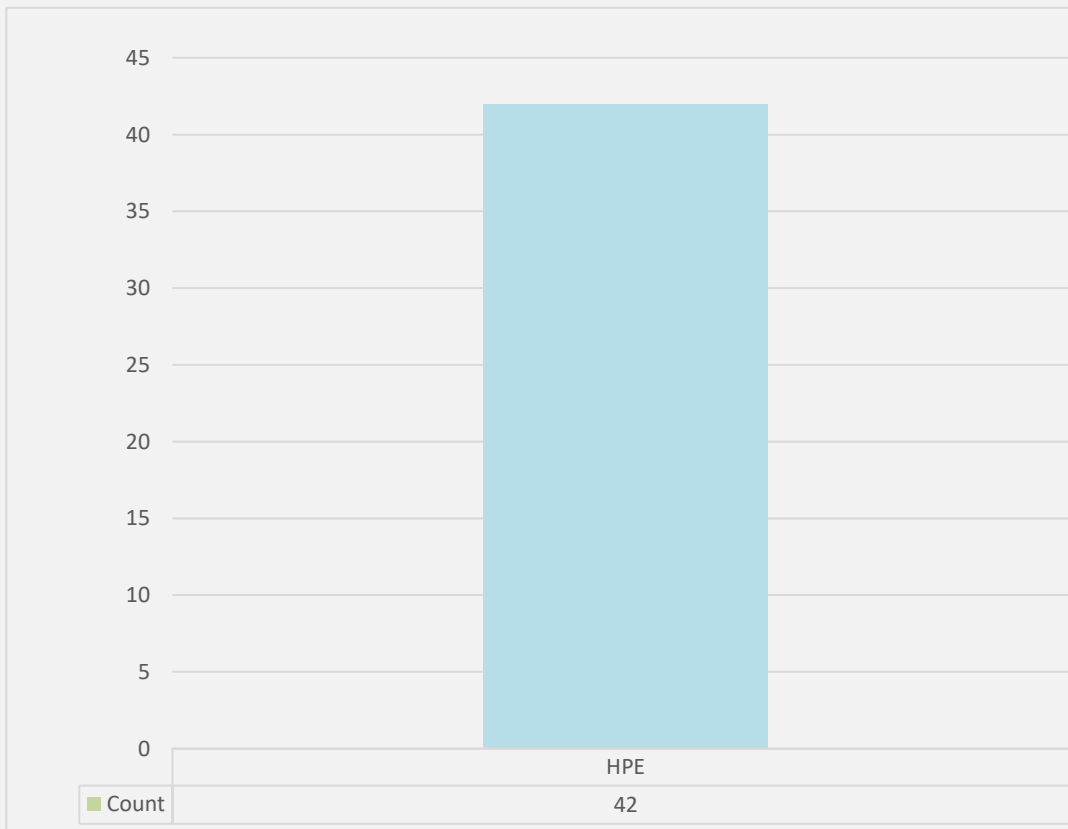
Product-wise Released EOS/EOL Count



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

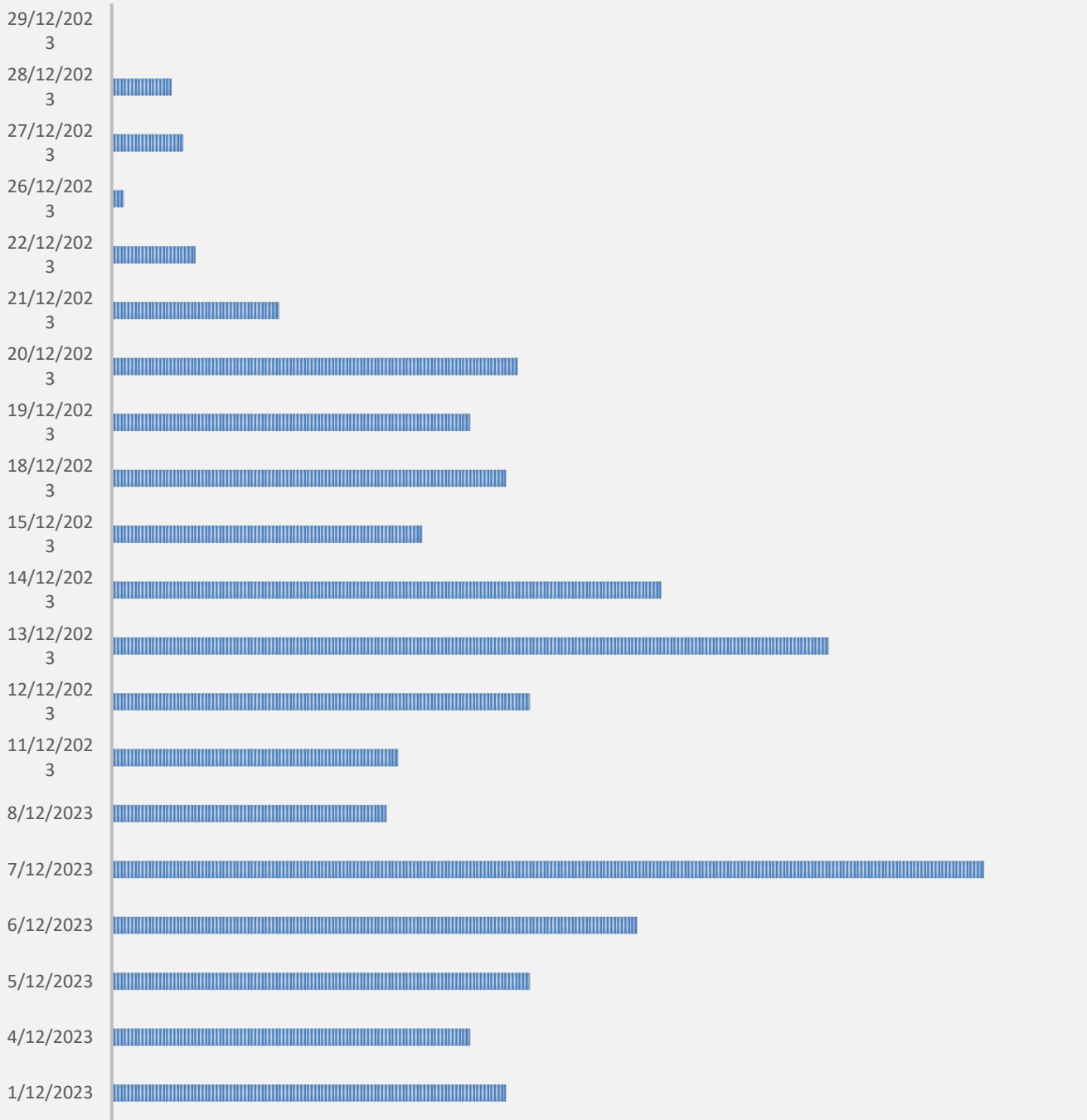


Critical CVE Count



Date-wise Released Vulnerabilities Count, Fortnightly Summarized

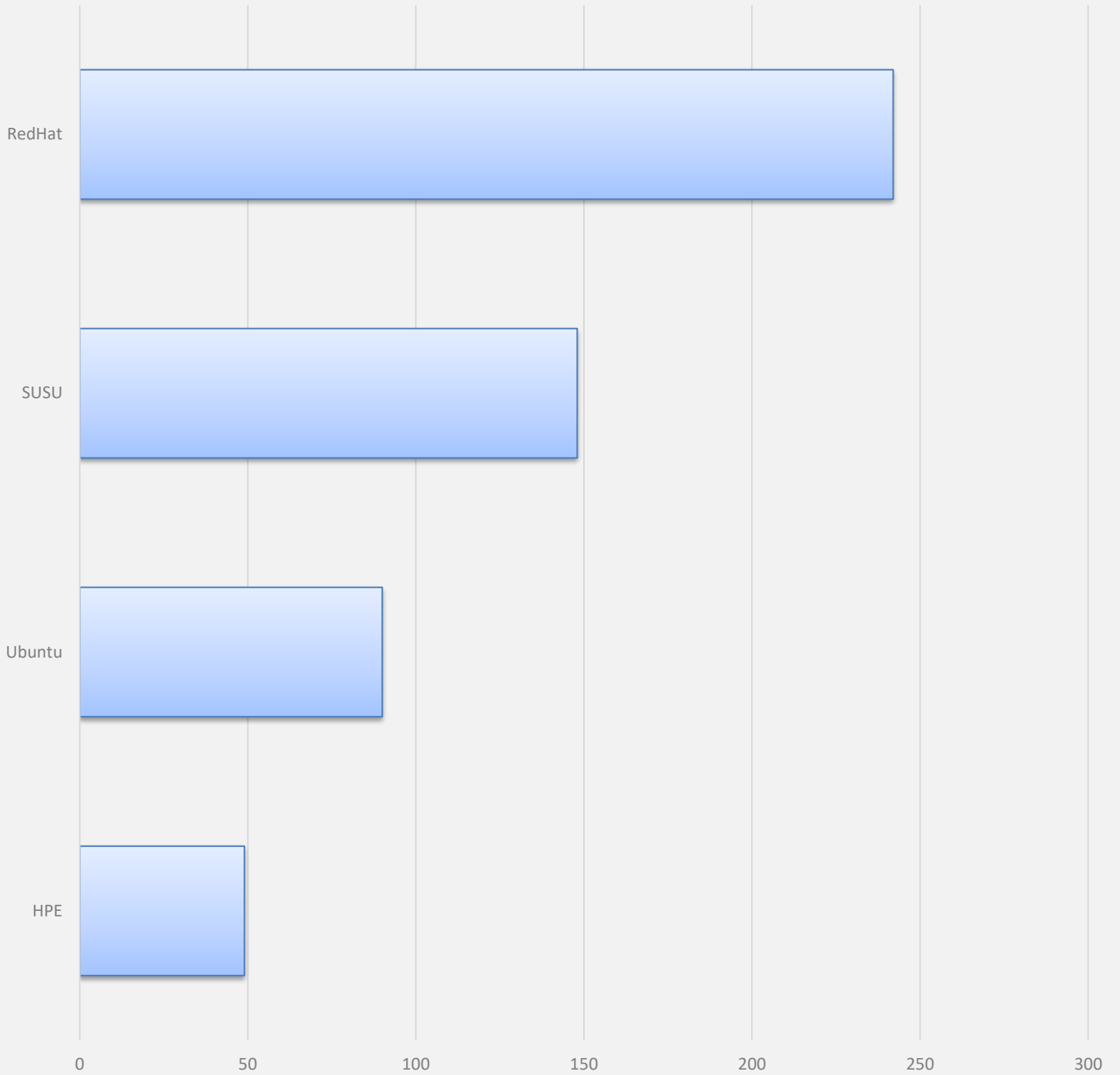
■ Count



0 10 20 30 40 50 60 70 80

	1/12/2023	4/12/2023	5/12/2023	6/12/2023	7/12/2023	8/12/2023	11/12/2023	12/12/2023	13/12/2023	14/12/2023	15/12/2023	18/12/2023	19/12/2023	20/12/2023	21/12/2023	22/12/2023	26/12/2023	27/12/2023	28/12/2023	29/12/2023
Count	33	30	35	44	73	23	24	35	60	46	26	33	30	34	14	7	1	6	5	0

Product-wise Chart for CVE



	HPE	Ubuntu	SUSU	RedHat
Count	49	90	148	242

Count

TOP VULNERABILITIES OF THE MONTH

DATE	CVE ID	Vendor	Product	Summary	Recommendation
01-Dec	CVE-2020-12912 CVE-2020-8694 CVE-2020-8695	SUSU	Containers Module 12 SUSE Linux Enterprise High-Performance Computing 12 SP2 SUSE Linux Enterprise High Performance Computing 12 SP3 SUSE Linux Enterprise High Performance Computing 12 SP4 SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise Server 12 SUSE Linux Enterprise Server 12 SP1 SUSE Linux Enterprise Server 12 SP2	Security update for containerd, docker, runc	Updates are available; please see the reference link below: https://www.suse.com/support/update/announcement/2023/suse-su-20234625-1/
11-Dec	CVE-2023-5868 CVE-2023-5869 CVE-2023-5870 CVE-2023-39417	RedHat	Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for ARM 64 8 aarch64	postgresql:12 security update	Updates are available; please see the reference link below: https://access.redhat.com/errata/RHSA-2023:7714
14-Dec	CVE-2023-22045 CVE-2023-22041 CVE-2023-22036 CVE-2023-22081 CVE-2023-46604 CVE-2023-22049	HPE	HPE Intelligent Management Center (iMC) - Prior to 7.3 E0710H02	HPE Intelligent Management Center, Multiple Vulnerabilities	Updates are available; please see the reference link below: https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbrnw04574en_us
20-Dec	"CVE-2022-24834 CVE-2023-32002 CVE-2023-38552"	HPE	HPE Unified OSS Console (UOC) - Prior to v3.1.0	HPE Unified OSS Console, Multiple Vulnerabilities	Updates are available; please see the reference link below: https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbmu04573en_us
22-Dec	CVE-2023-6377	SUSU	Security update for xorg-x11-server	Basesystem Module 15-SP4 Development Tools Module 15-SP4 openSUSE Leap 15.4 SUSE Linux Enterprise Desktop 15 SP4 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP4	Updates are available; please see the reference link below: https://www.suse.com/support/update/announcement/2023/suse-su-20234949-1/

Disclaimer: The information in this document is subject to change without notice and should not be construed as a commitment by Satrix Information Security (P) Ltd. Satrix 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 Satrix 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 Satrix 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 Satrix, 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 © Copyright 2013-2022 Satrix. All rights reserved.

Limitation of Liability: IN NO EVENT SHALL Satrix, Satrix 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 Satrix 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 / Satrix Information Security Incorporation

UK/EU / Satrix Info Security Ltd

MEA / Satrix Information Security DMCC

India / Satrix 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@satrix.com

www.satrix.com

