SECURITY INTELLIGENCE ADVISORY

1st Nov 2023 - 30th Nov 2023

INTENT

This report is intended to help quantify the scope of that risk 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.

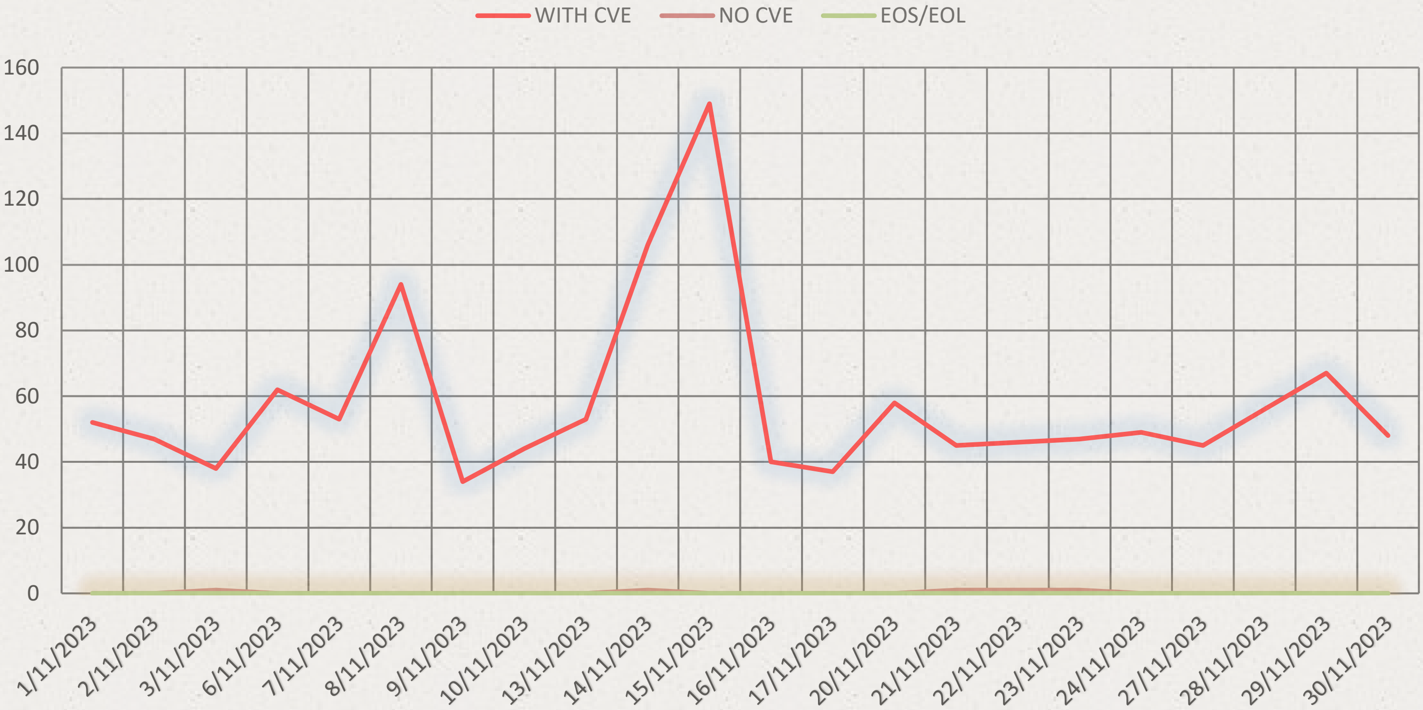
One effective way to stay on top of these vulnerabilities is by conducting regular vulnerability assessments. These periodic assessments cover your entire IT infrastructure and help you identify new threats that may have emerged. This proactive practice enables you to stay abreast of the current state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

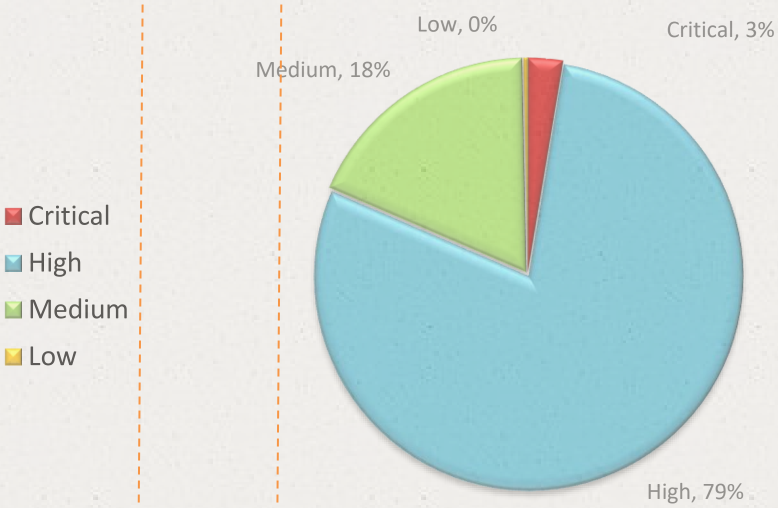
EXECUTIVE SUMMARY

Overall Monthly Vulnerability Trend Chart



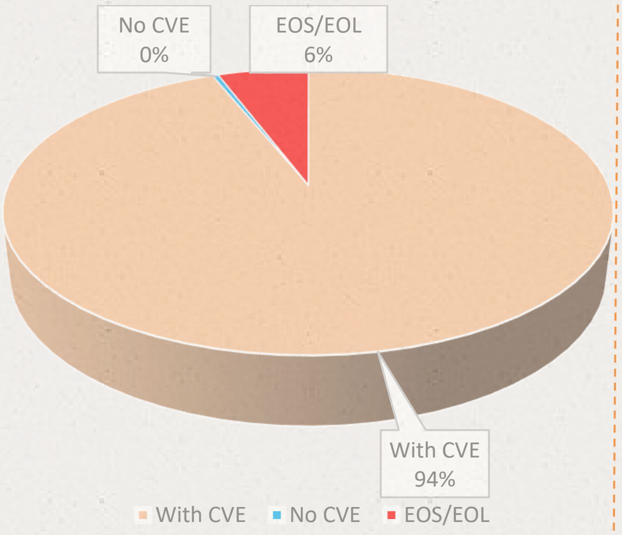
Released Vulnerabilities and Severity-wise Count

This graph presents threat levels based on vulnerabilities identified.

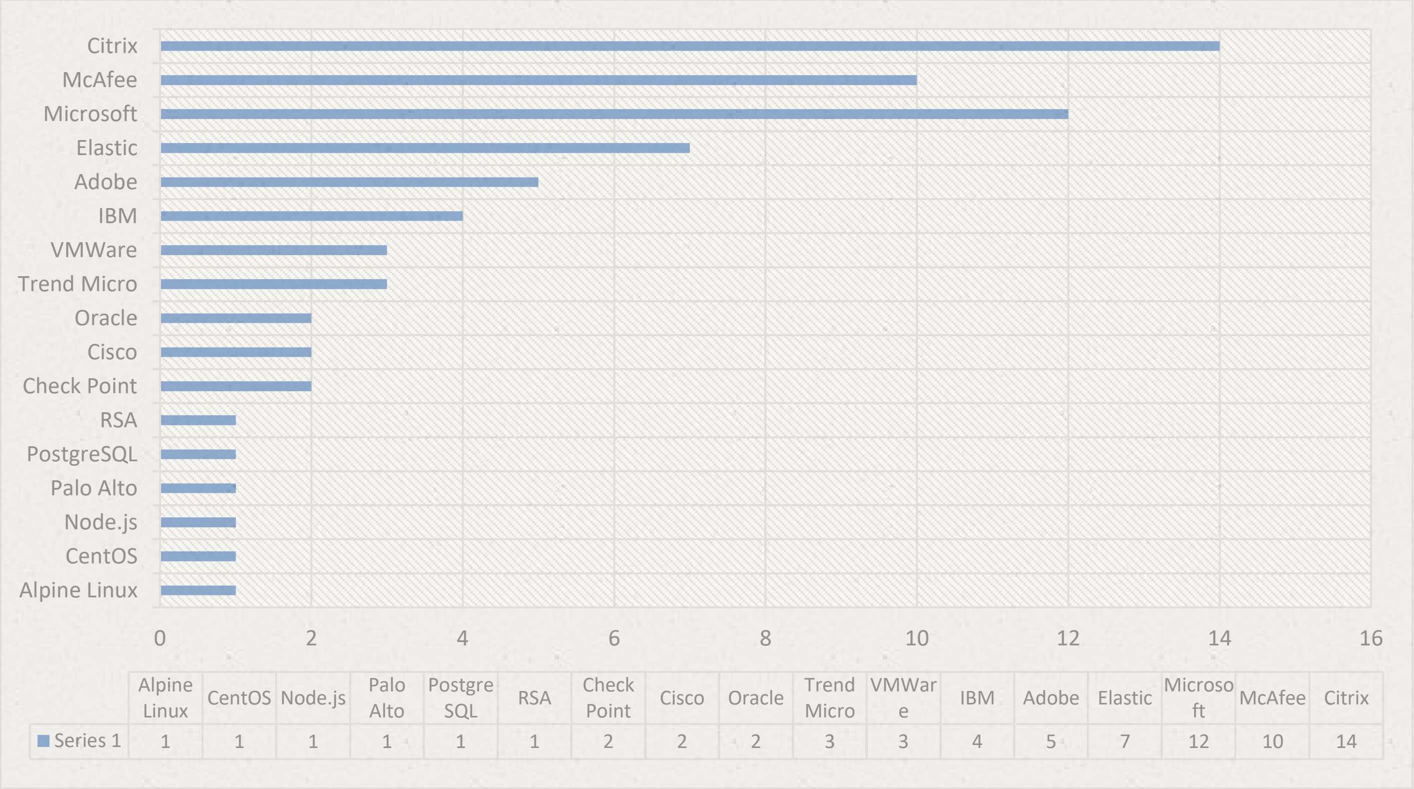


EXECUTIVE SUMMARY

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

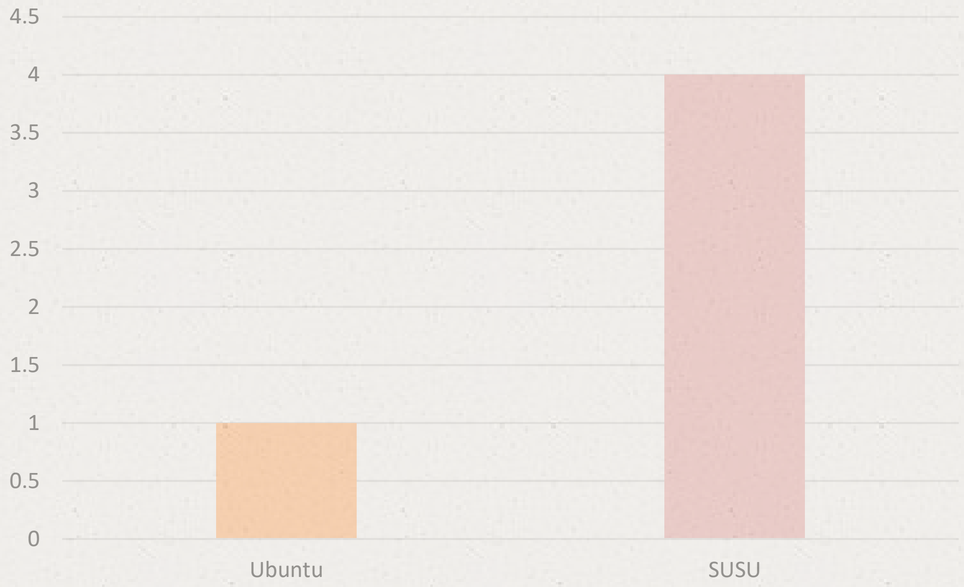


Product-wise Released EOS/EOL Count

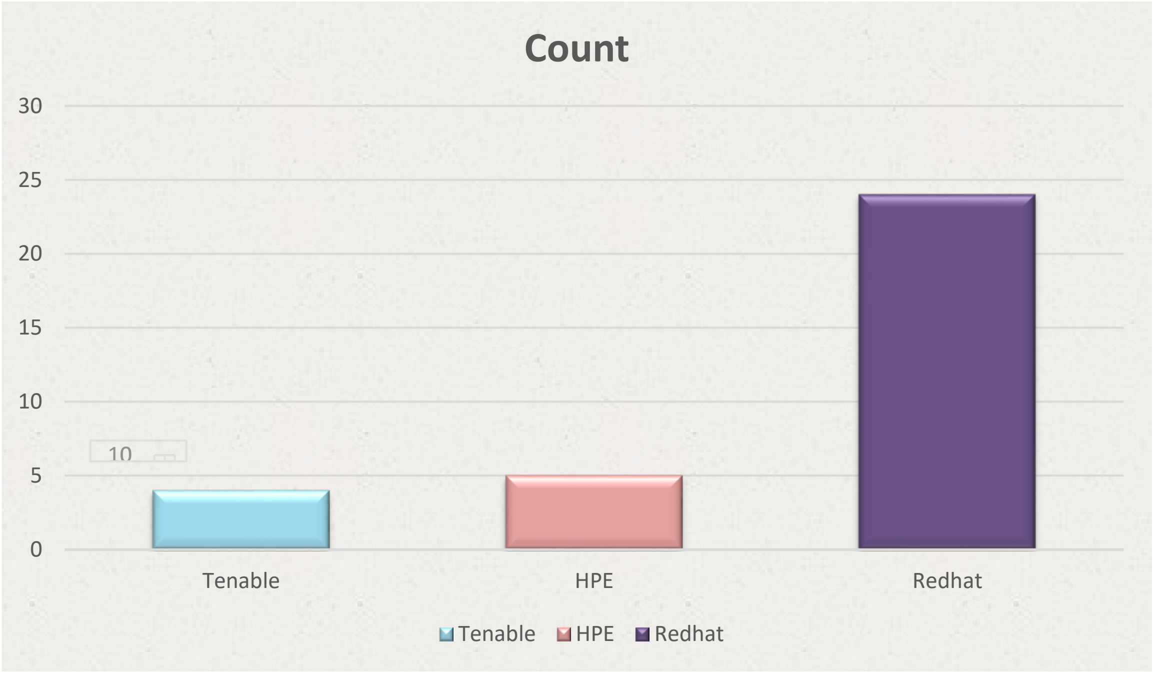


	Alpine Linux	CentOS	Node.js	Palo Alto	Postgre SQL	RSA	Check Point	Cisco	Oracle	Trend Micro	VMWar e	IBM	Adobe	Elastic	Microso ft	McAfee	Citrix
■ Series 1	1	1	1	1	1	1	2	2	2	3	3	4	5	7	12	10	14

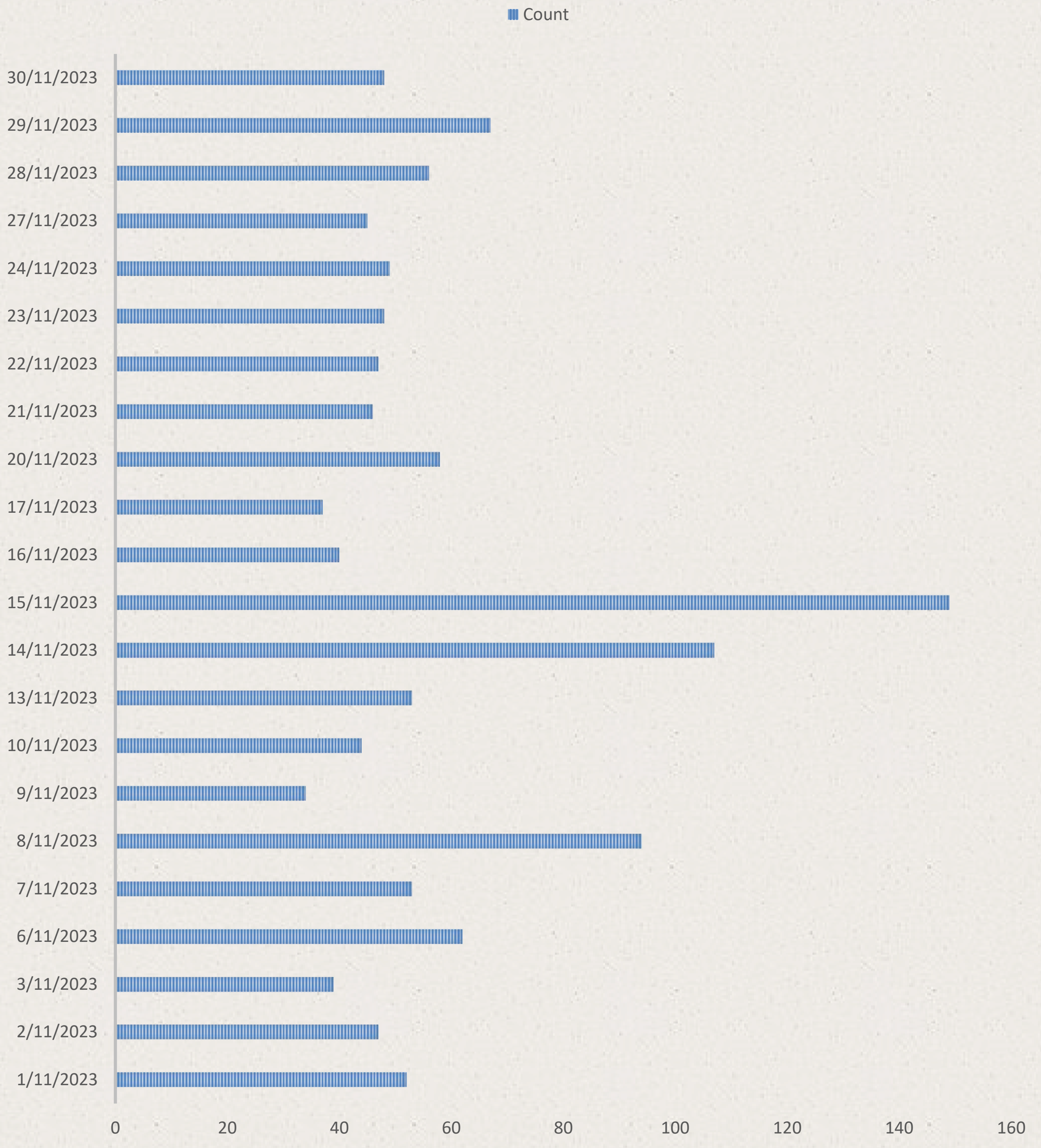
Product-wise Released Non-CVE ID or Zero Day Vulnerabilities Count



Critical CVE Count

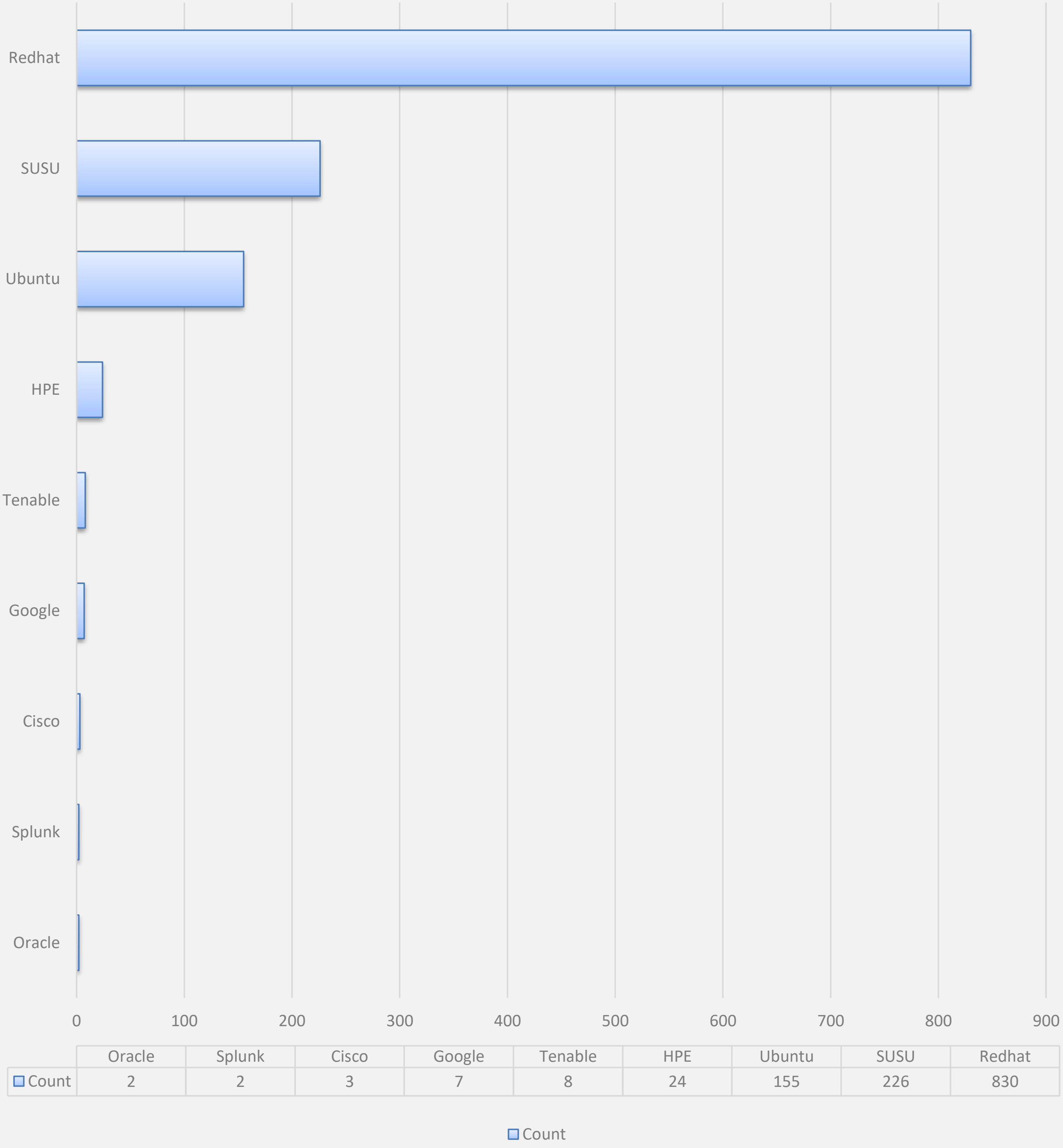


Date-wise Released Vulnerabilities Count, Fortnightly Summarized



	1/11/2023	2/11/2023	3/11/2023	6/11/2023	7/11/2023	8/11/2023	9/11/2023	10/11/2023	13/11/2023	14/11/2023	15/11/2023	16/11/2023	17/11/2023	20/11/2023	21/11/2023	22/11/2023	23/11/2023	24/11/2023	27/11/2023	28/11/2023	29/11/2023	30/11/2023
▥ Count	52	47	39	62	53	94	34	44	53	107	149	40	37	58	46	47	48	49	45	56	67	48

Product-wise chart for CVE



	Oracle	Splunk	Cisco	Google	Tenable	HPE	Ubuntu	SUSU	Redhat
□ Count	2	2	3	7	8	24	155	226	830

TOP VULNERABILITIES OF THE MONTH

DATE	CVE ID	Vendor	Product	Summary	Recommendation
02-11-23	CVE-2023-46846 CVE-2023-46847 CVE-2023-46848	RedHat	Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux for IBM z Systems 9 s390x	Squid is a high-performance proxy caching server for web clients, supporting FTP, Gopher, and HTTP data objects.	Updates available; please click the reference link to view them: https://access.redhat.com/errata/RHSA-2023:6266
07-11-23	CVE-2023-30908 CVE-2023-30909	HPE	HPE OneView 7.00.00 HPE OneView 7.10.00 HPE OneView 7.20.00 HPE OneView 8.00.00 HPE OneView 8.10.00 HPE OneView 8.20.00 HPE OneView 8.30.00 HPE OneView 8.40.00	Potential security vulnerabilities have been identified in Hewlett Packard Enterprise OneView and HPE OneView Global Dashboard (OVGD) Software. These vulnerabilities could be remotely exploited to allow authentication bypass.	Updates available; please click the reference link to view them: https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04538en_us
09-11-23	CVE-2020-22218 CVE-2023-22067 CVE-2023-22081 CVE-2023-46604	Redhat	Red Hat OpenShift Container Platform 3.11 x86_64	Red Hat OpenShift Container Platform 3.11 x86_64	Updates available; please click the reference link to view them: https://access.redhat.com/errata/RHSA-2023:6866
	CVE-2023-46604	Redhat	Red Hat Fuse 1 x86_64	An update is now available for Red Hat JBoss Fuse 6.3 and Red Hat JBoss A-MQ 6.3.	Updates available; please click the reference link to view them: https://access.redhat.com/errata/RHSA-2023:6849
15-11-23	CVE-2023-46846 CVE-2023-46847	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	Squid is a high-performance proxy caching server for web clients, supporting FTP, Gopher, and HTTP data objects.	Updates available; please click the reference link to view them: https://access.redhat.com/errata/RHSA-2023:7213
30-11-23	CVE-2023-30912	HPE	HPE OneView All versions prior to 6.60.06, 8.60.00	A potential security vulnerability has been identified in Hewlett Packard Enterprise OneView Software. This vulnerability could be exploited to allow remote code execution.	Updates available; please click the reference link to view them: https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04548en_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 © Copyright 2013-2022 Sattrix. All rights reserved.

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 (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