SECURITY INTELLIGENCE ADVISORY

01st Sep 2024 – 30th Sep 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.

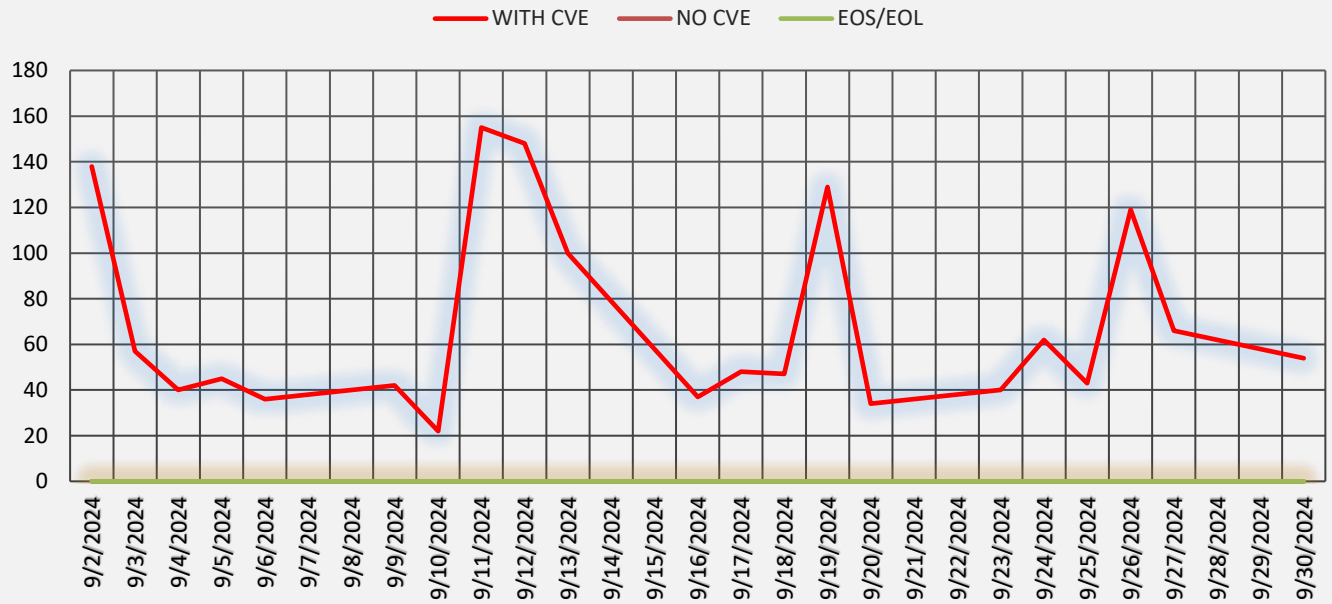
One effective way to stay on top of these vulnerabilities is by conducting regular vulnerability assessments. These periodic assessments cover your entire IT infrastructure and help you identify new threats that may have emerged. This proactive practice enables you to stay abreast of the current state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

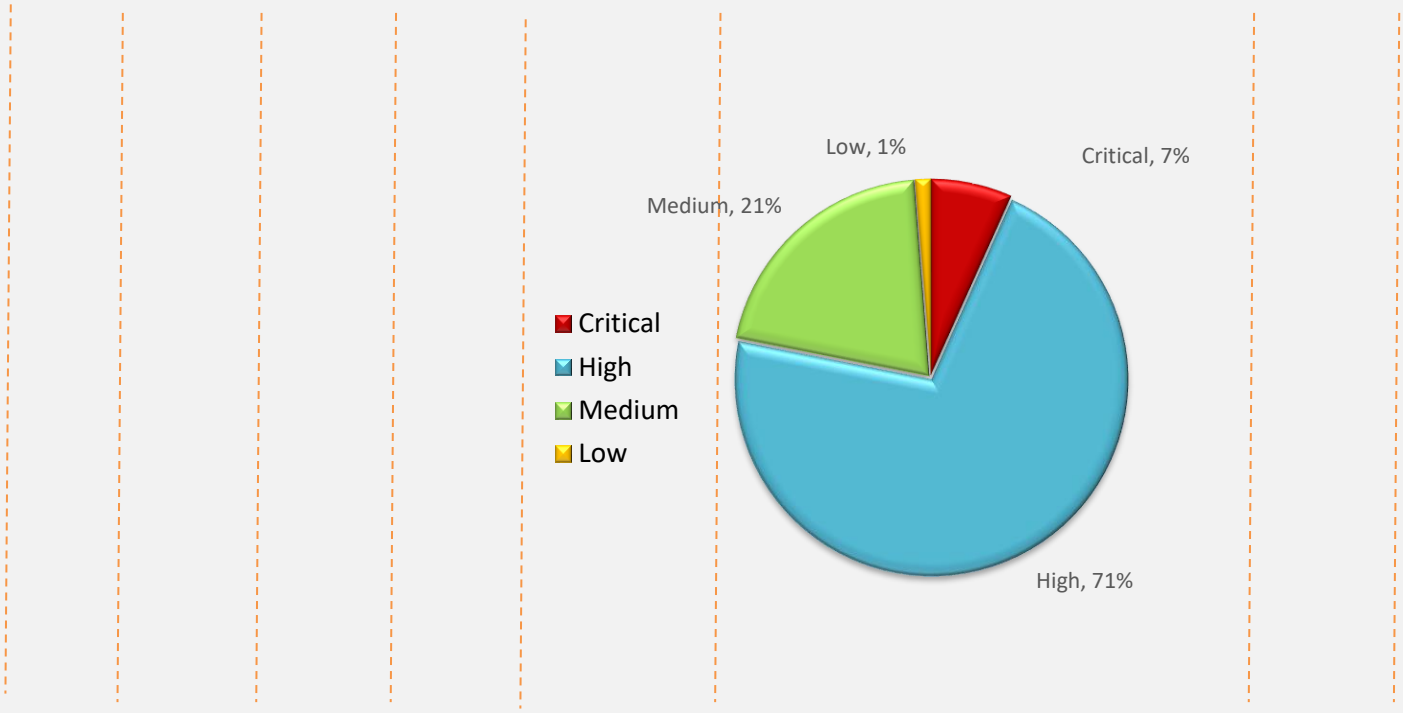
EXECUTIVE SUMMARY

Overall Monthly Vulnerability Trend Chart



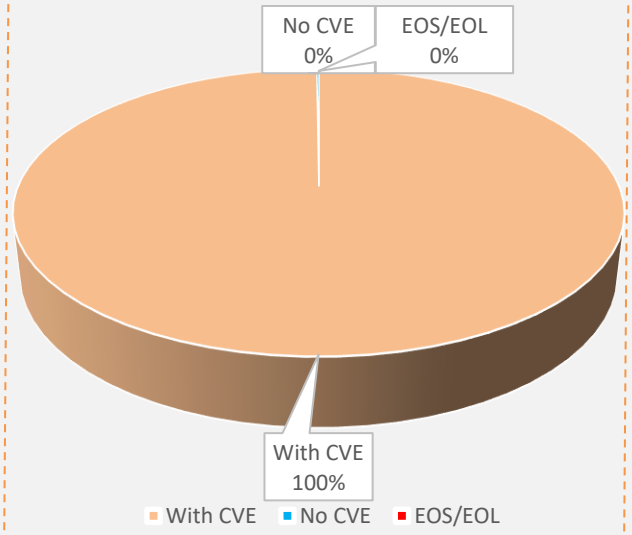
Released Vulnerabilities and Severity Count:

This graph presents threat levels based on vulnerability identified.

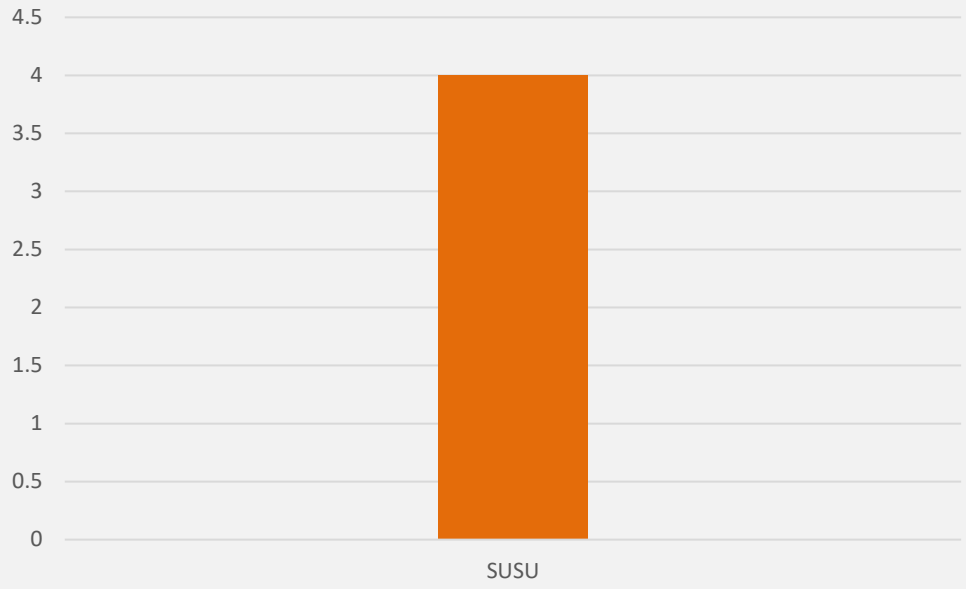


EXECUTIVE SUMMARY

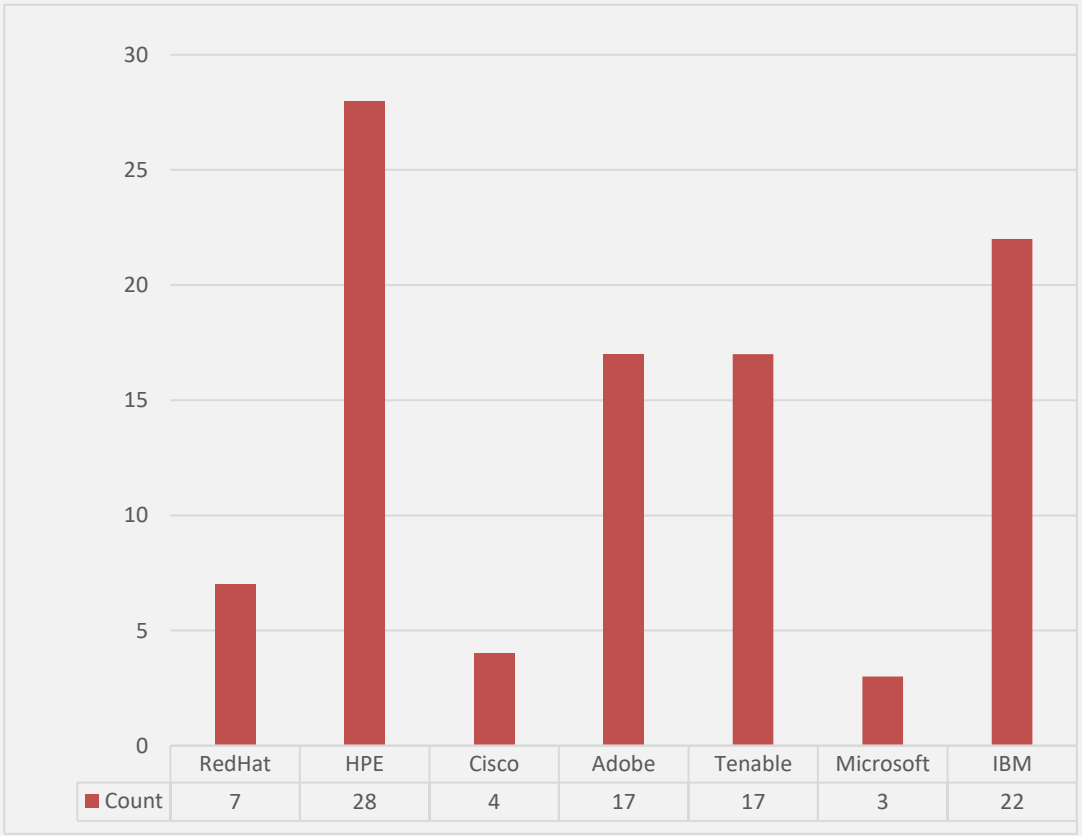
This graph presents the total vulnerabilities released, including zero-day vulnerability and EOS/EOL, with their count.



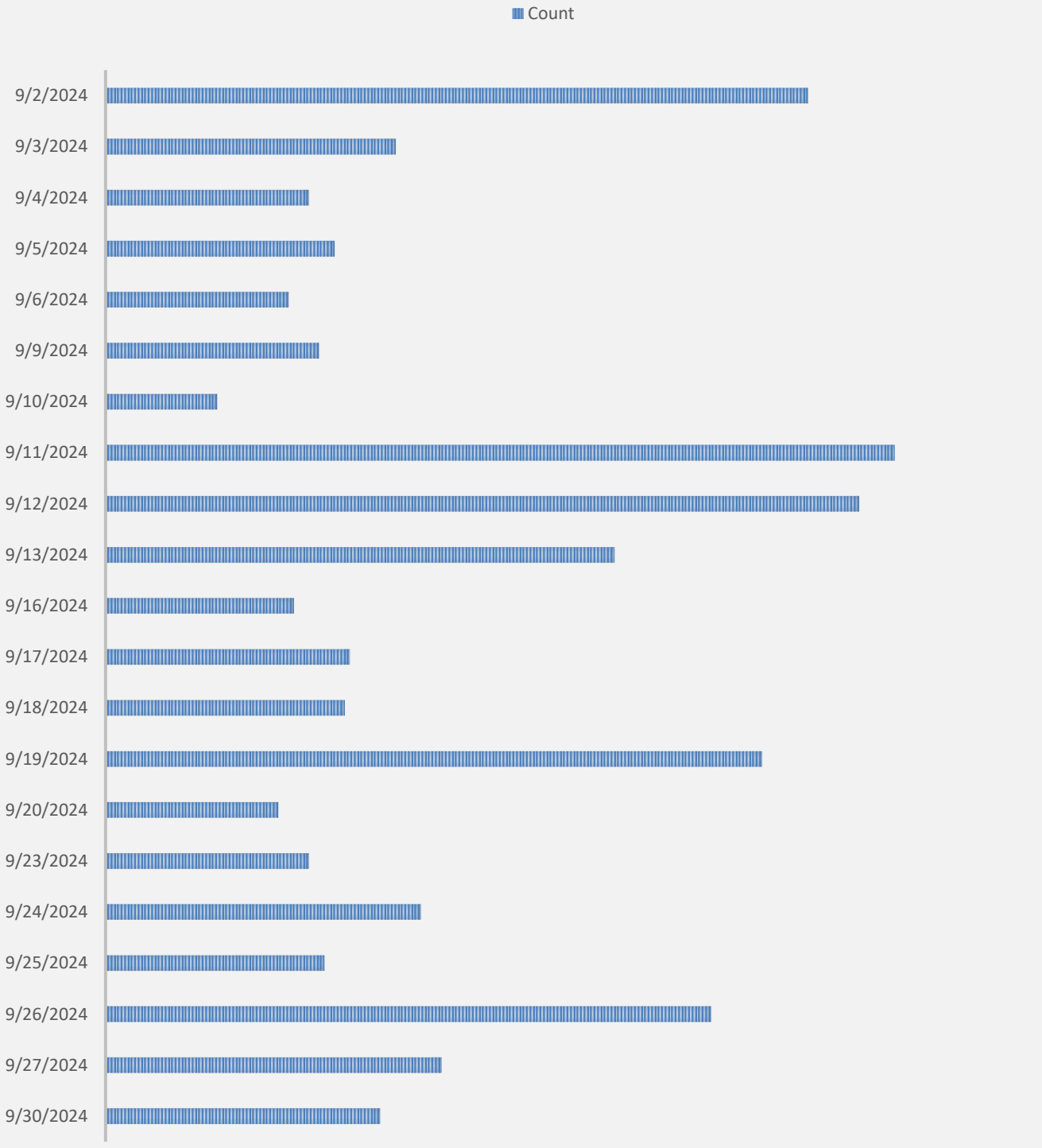
Product-wise Released Non-CVE ID or Zero Day Vulnerabilities Count



Critical CVE Count

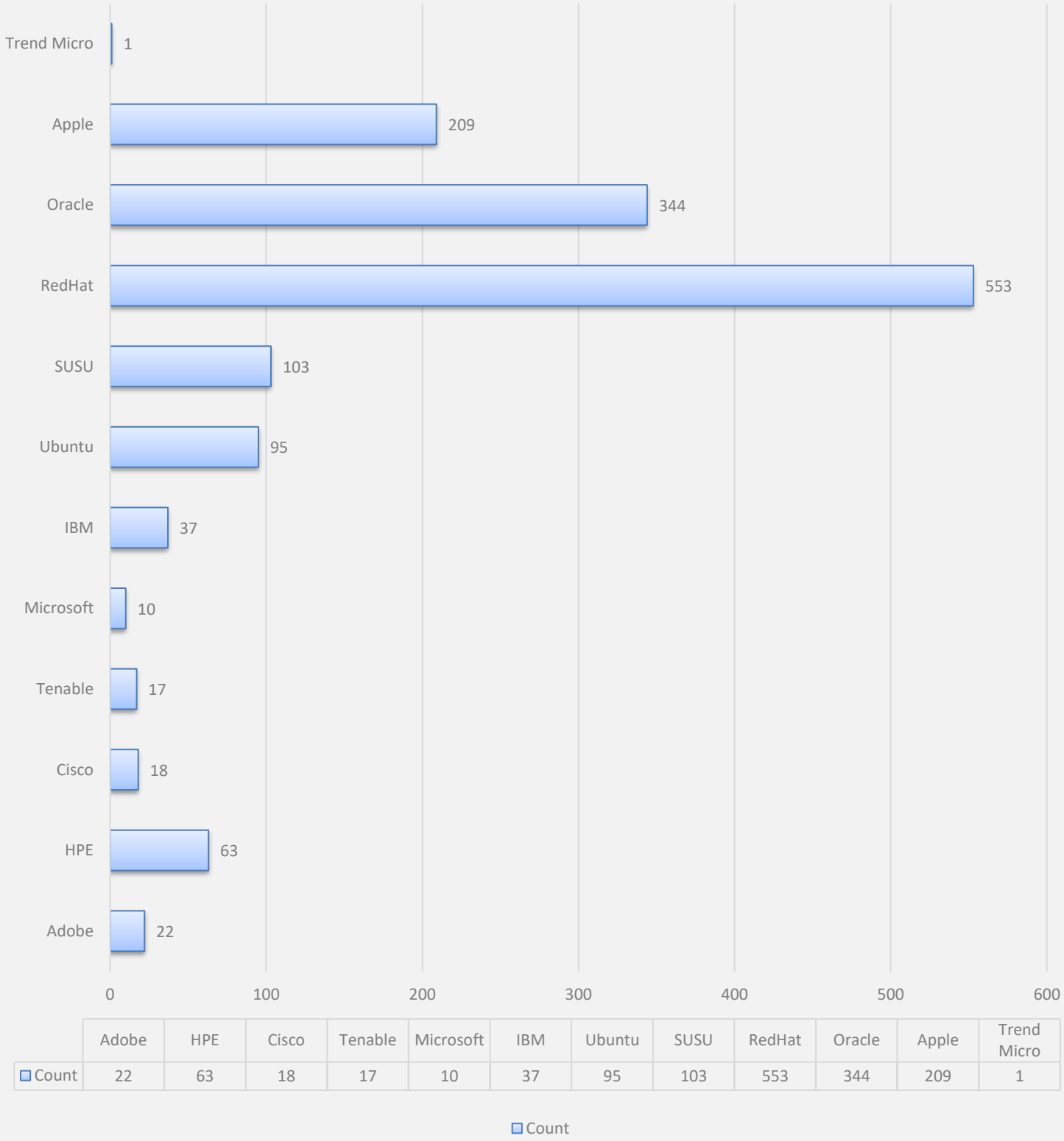


Date-wise Released Vulnerabilities Count, Fortnightly Summarized



	9/30/2024	9/27/2024	9/26/2024	9/25/2024	9/24/2024	9/23/2024	9/20/2024	9/19/2024	9/18/2024	9/17/2024	9/16/2024	9/13/2024	9/12/2024	9/11/2024	9/10/2024	9/9/2024	9/6/2024	9/5/2024	9/4/2024	9/3/2024	9/2/2024
Count	54	66	119	43	62	40	34	129	47	48	37	100	148	155	22	42	36	45	40	57	138

Product-wise Chart for CVE



	Adobe	HPE	Cisco	Tenable	Microsoft	IBM	Ubuntu	SUSU	RedHat	Oracle	Apple	Trend Micro
Count	22	63	18	17	10	37	95	103	553	344	209	1

TOP VULNERABILITIES OF THE MONTH

CVE ID	Vendor	Severity	Summary
CVE-2023-45288 CVE-2023-45290 CVE-2023-49569 CVE-2024-24783 CVE-2024-24785 CVE-2024-24786 CVE-2024-24788	RedHat	Critical	The Red Hat OpenShift Builds 1.1.0 General Availability
CVE-2021-41617 CVE-2021-28041 CVE-2021-31580 CVE-2016-20012 CVE-2021-36368 CVE-2023-25136 CVE-2023-48795 CVE-2023-51384 CVE-2023-51385 CVE-2023-38408	HPE	Critical	HP-UX Secure Shell, Multiple Vulnerabilities
CVE-2024-20439 CVE-2024-20440 CWE-532 CWE-912	Cisco	Critical	Cisco Smart Licensing Utility Vulnerabilities
CVE-2024-39377 CVE-2024-41871	Adobe	Critical	Security Updates Available for Adobe Media Encoder | APSB24-53
CVE-2024-39380 CVE-2024-41859 CVE-2024-39381	Adobe	Critical	Security Updates Available for Adobe After Effects | APSB24-55
CVE-2024-41857 CVE-2024-34121 CVE-2024-43758 CVE-2024-43759 CVE-2024-41856 CVE-2024-45111	Adobe	Critical	Security Updates Available for Adobe Illustrator | APSB24-66
CVE-2024-43756 CVE-2024-43760 CVE-2024-45108 CVE-2024-45109	Adobe	Critical	Security update available for Adobe Photoshop | APSB24-72
CVE-2024-41869 CVE-2024-45112	Adobe	Critical	Security update available for Adobe Acrobat and Reader | APSB24-70
CVE-2024-6119 CVE-2024-45491 CVE-2024-45492	Tenable	Critical	Nessus Version 10.8.3 Fixes Multiple Vulnerabilities
CVE-2024-6119 CVE-2024-45491 CVE-2024-45492	Tenable	Critical	Nessus Version 10.7.6 Fixes Multiple Vulnerabilities
CVE-2024-6119 CVE-2024-45491 CVE-2024-45493	Tenable	Critical	Nessus Agent Version 10.7.3 Fixes Multiple Vulnerabilities
CVE-2024-38119	Microsoft	Critical	Windows Network Address Translation (NAT) Remote Code Execution Vulnerability
CVE-2024-38183	Microsoft	Critical	GroupMe Elevation of Privilege Vulnerability
CVE-2024-43460	Microsoft	Critical	Dynamics 365 Business Central Elevation of Privilege Vulnerability
CVE-2024-28757 CVE-2023-52426 CVE-2023-52425 CVE-2022-43680 CVE-2012-0876 CVE-2021-3520 CVE-2024-0727 CVE-2023-6237 CVE-2023-5678 CVE-2023-5363 CVE-2023-3446 CVE-2024-31497 CVE-2023-48795	HPE	Critical	HPE NonStop BackBox and QORESTOR products, multiple vulnerabilities

CVE-2023-39615 CVE-2023-46218 CVE-2023-38546 CVE-2023-28322 CVE-2021-22925			
CVE-2024-24787	IBM	Critical	Security Bulletin: Vulnerabilities in Node.js, AngularJS, Golang Go, libcURL, PostgreSQL, Linux kernel might affect IBM Spectrum Protect Plus
CVE-2023-39320	IBM	Critical	Multiple Vulnerabilities in IBM Cloud Pak for Multicloud Management
CVE-2020-10673 CVE-2020-10672 CVE-2017-17485 CVE-2018-14718 CVE-2018-14721 CVE-2019-12384	IBM	Critical	Vulnerabilities in FasterXML jackson-databind and other packages affect IBM watsonx.data
CVE-2024-6119 CVE-2024-45491 CVE-2024-45492 CVE-2024-6197 CVE-2024-7264 CVE-2024-8096 CVE-2024-34459 CVE-2024-9158	Tenable	Critical	Nessus Network Monitor 6.5.0 Fixes Multiple Vulnerabilities
CVE-2020-24750 CVE-2020-24616 CVE-2020-36185 CVE-2020-36183 CVE-2020-36182 CVE-2020-36181 CVE-2020-36179 CVE-2020-36180 CVE-2020-36184 CVE-2020-14195 CVE-2021-20190 CVE-2020-36186 CVE-2020-36187 CVE-2020-36188	IBM	Critical	Multiple vulnerabilities affect IBM Db2® on Cloud Pak for Data, and Db2 Warehouse on Cloud Pak for Data

Non-CVE ID or Zero Day Vulnerabilities Count:

SL. No	Title	Vendor	Severity	Summary
01	Security update for kubernetes1.24	SUSU	High	Containers Module 15-SP5 openSUSE Leap 15.5 openSUSE Leap 15.6 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP5
02	Security update for kubernetes1.28	SUSU	High	Containers Module 15-SP5 Containers Module 15-SP6 openSUSE Leap 15.4 openSUSE Leap 15.5 openSUSE Leap 15.6 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP4 SUSE Linux Enterprise High Performance Computing LTSS 15 SP4 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server 15 SP4 LTSS 15-SP4 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP6
03	Security update for kubernetes1.24	SUSU	High	openSUSE Leap 15.3 SUSE Enterprise Storage 7.1 SUSE Linux Enterprise High Performance Computing 15 SP3 SUSE Linux Enterprise High Performance Computing LTSS 15 SP3 SUSE Linux Enterprise Server 15 SP3 SUSE Linux Enterprise Server 15 SP3 LTSS 15-SP3 SUSE Linux Enterprise Server for SAP Applications 15 SP3

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**