SECURITY INTELLIGENCE ADVISORY

01st August 2024 – 31st August 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.

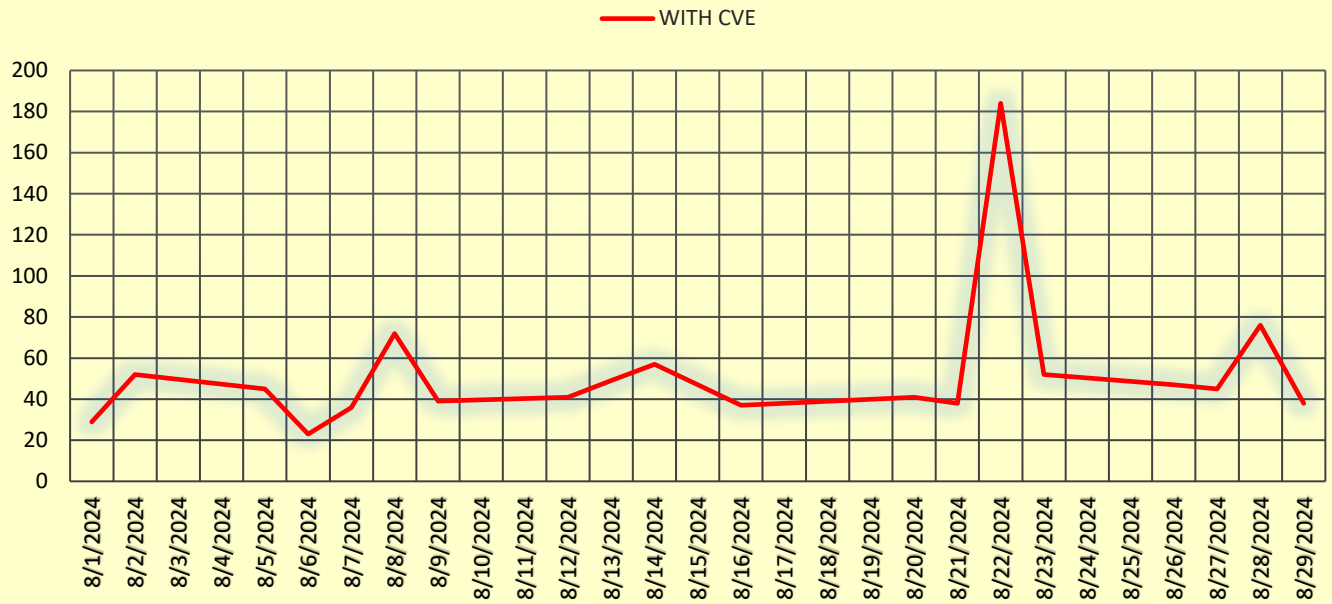
One effective way to stay on top of these vulnerabilities is by conducting regular vulnerability assessments. These periodic assessments cover your entire IT infrastructure and help you identify new threats that may have emerged. This proactive practice enables you to stay abreast of the current state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

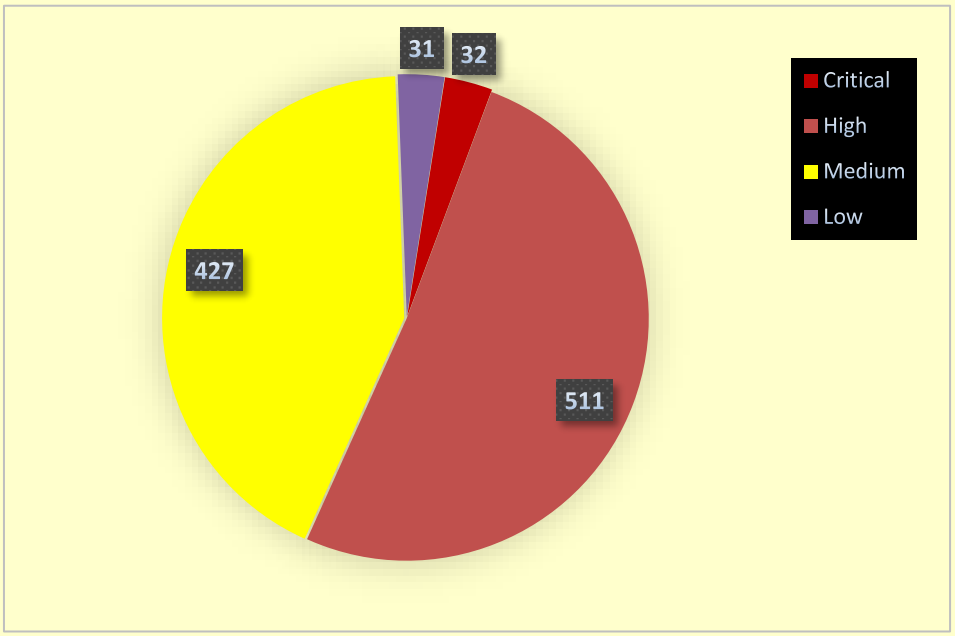
EXECUTIVE SUMMARY

Overall Monthly Vulnerability Trend Chart



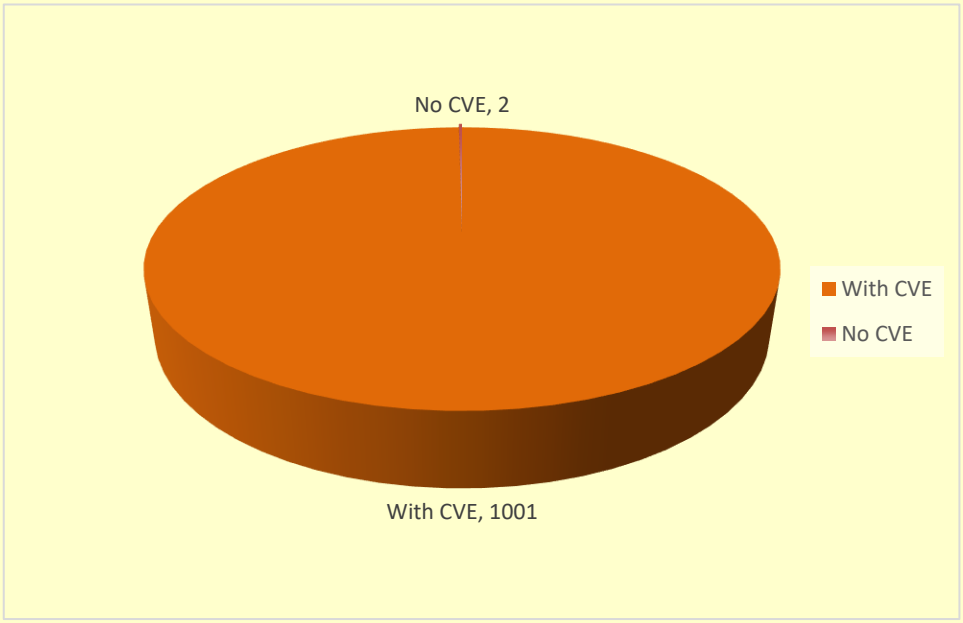
Released Vulnerabilities and Severity Count:

This graph presents threat levels based on vulnerability identified.

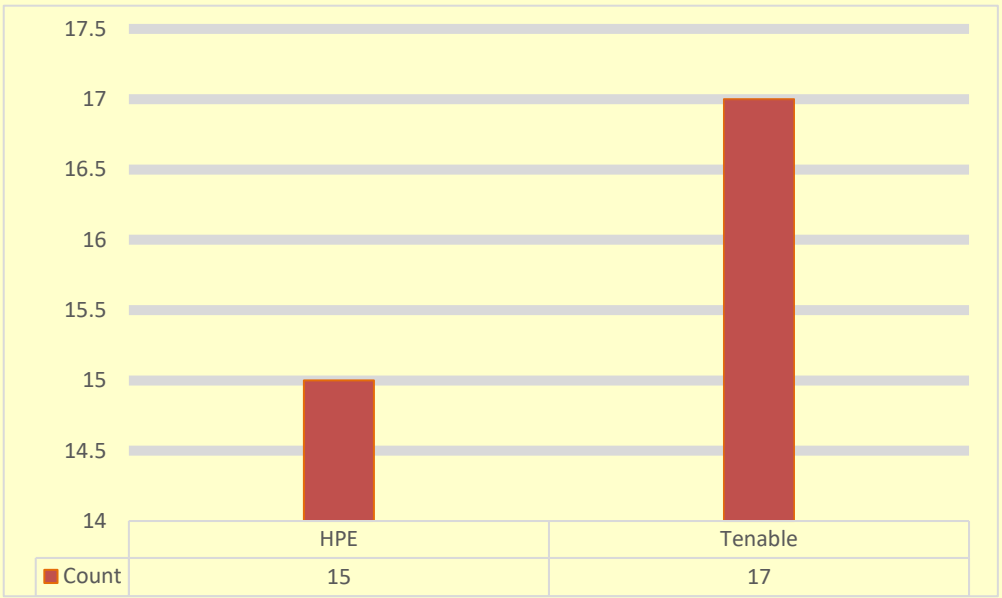


EXECUTIVE SUMMARY

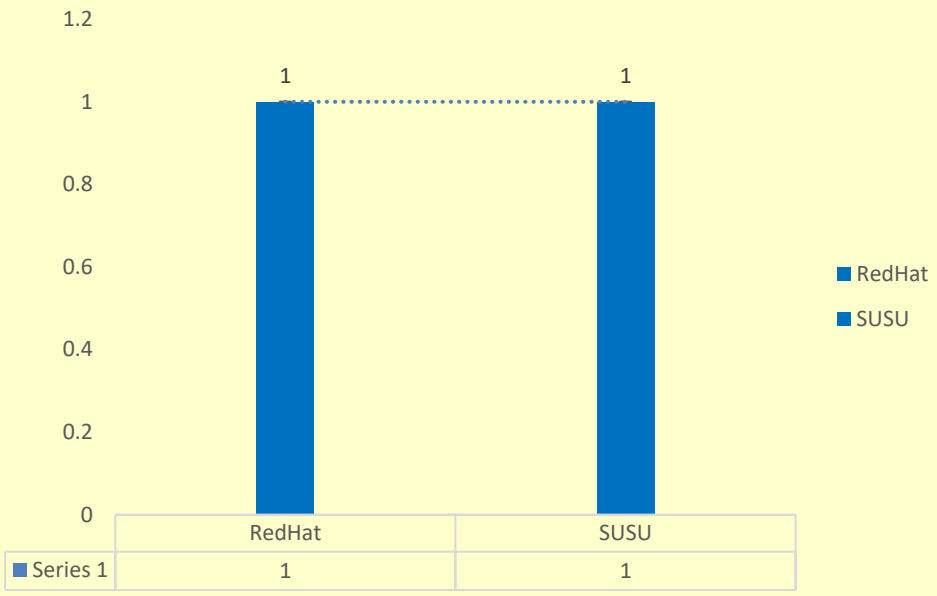
This graph presents the total vulnerabilities released, including zero-day vulnerability with their count.



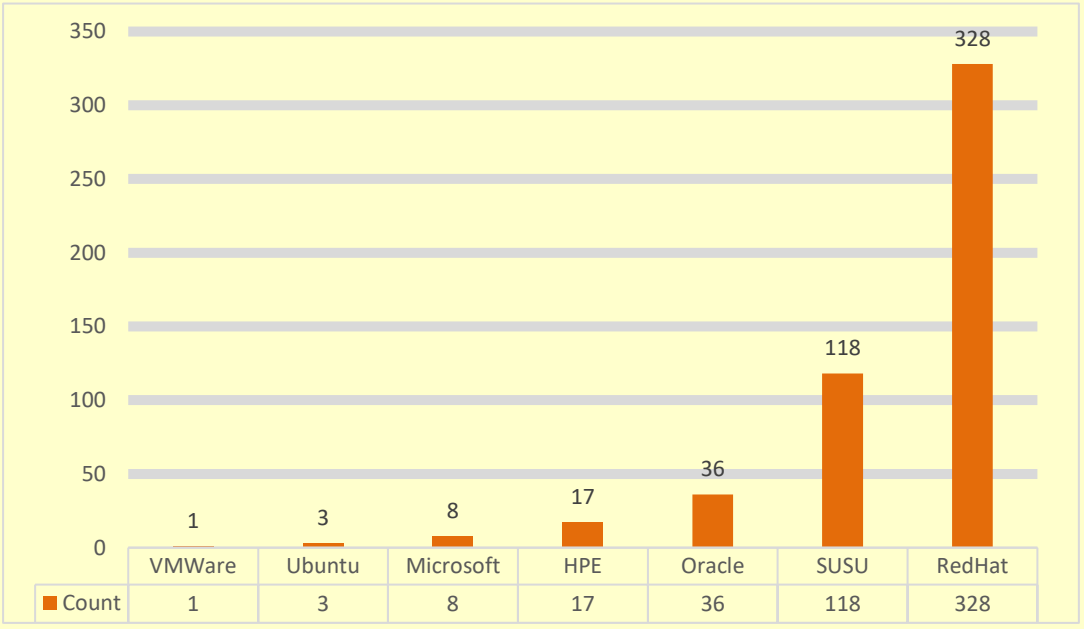
Critical CVE Count: -



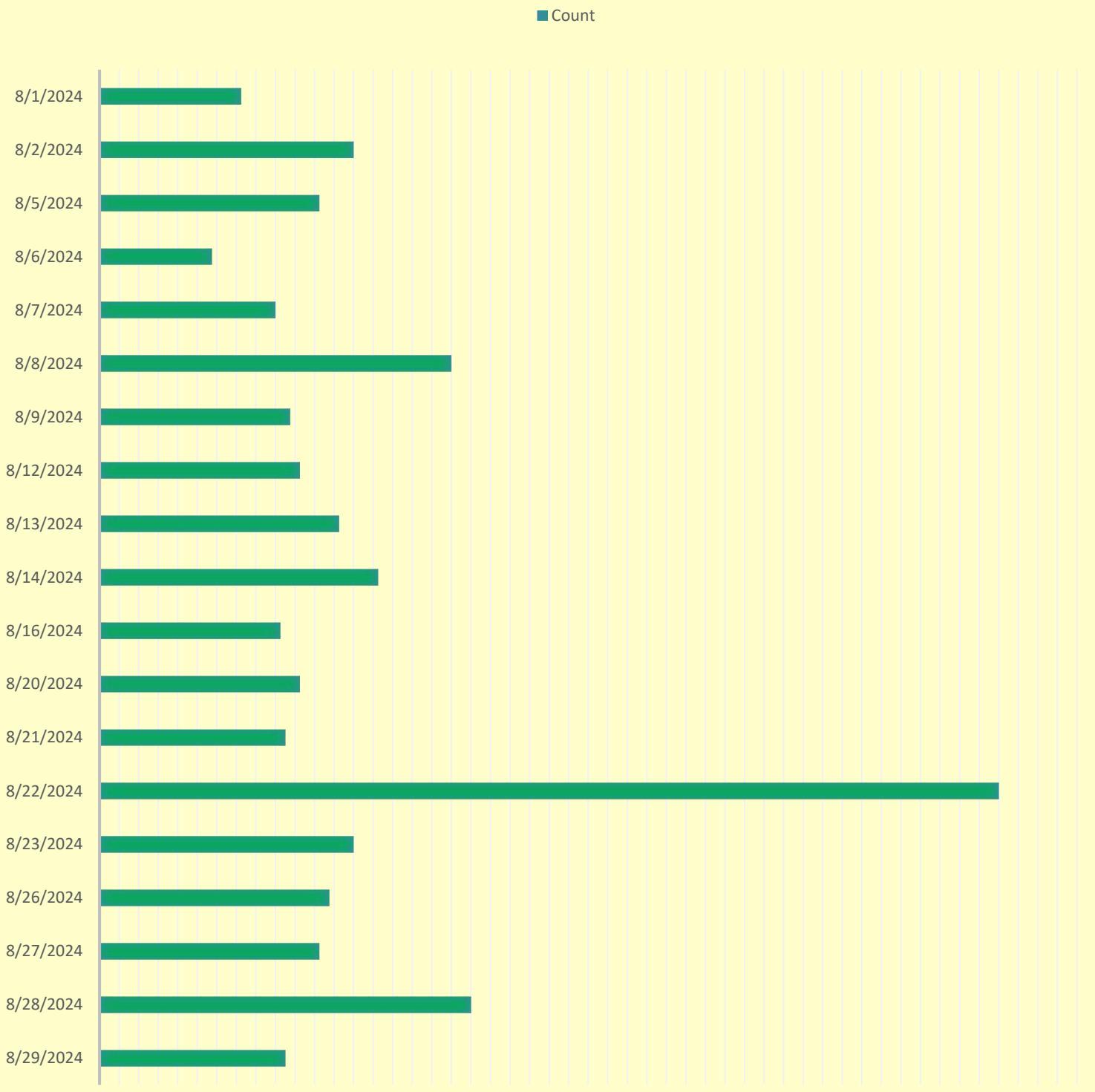
Product-wise Released Non-CVE ID or Zero Day Vulnerabilities Count



HIGH CVE Count: -

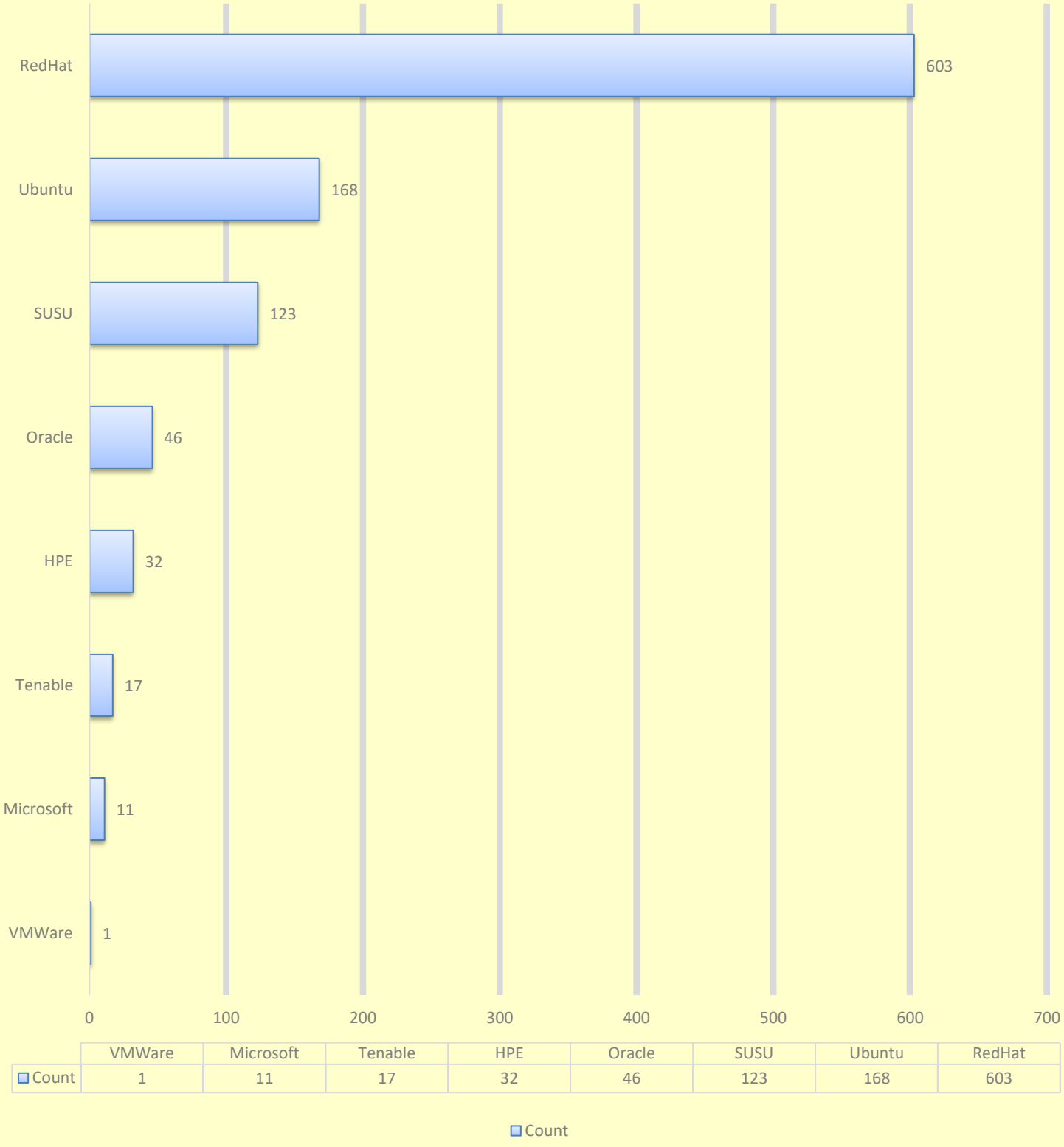


Date-wise Released Vulnerabilities Count, Fortnightly Summarized



	8/29/2024	8/28/2024	8/27/2024	8/26/2024	8/23/2024	8/22/2024	8/21/2024	8/20/2024	8/16/2024	8/14/2024	8/13/2024	8/12/2024	8/9/2024	8/8/2024	8/7/2024	8/6/2024	8/5/2024	8/2/2024	8/1/2024
Count	38	76	45	47	52	184	38	41	37	57	49	41	39	72	36	23	45	52	29

Product-wise Chart for CVE



	VMWare	Microsoft	Tenable	HPE	Oracle	SUSU	Ubuntu	RedHat
Count	1	11	17	32	46	123	168	603

VULNERABILITITIES OF THIS MONTH

Date	Sr. #	CVE ID	Vendor	Severity	Summary	Recommendations
1-Aug	01	CVE-2023-7104 CVE-2023-45288 CVE-2023-45290 CVE-2024-24783 CVE-2024-24784 CVE-2024-24785 CVE-2024-24786	RedHat	High	Run Once Duration Override Operator for Red Hat OpenShift 1.1.1 for RHEL 9	Updates are available please see below reference link: https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04558en_us&docLocale=en_US
	02	CVE-2023-45290 CVE-2024-24783 CVE-2024-24784 CVE-2024-24785 CVE-2024-24786	RedHat	Medium	Kube Descheduler Operator for Red Hat OpenShift 5.0.1 for RHEL 9	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:3617
	03	CVE-2023-45288 CVE-2023-45290 CVE-2024-24783 CVE-2024-24784 CVE-2024-24785 CVE-2024-24786	RedHat	Medium	Secondary Scheduler Operator for Red Hat OpenShift 1.3.0 for RHEL 9	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:3637
	04	CVE-2023-7104 CVE-2023-45288 CVE-2023-45290 CVE-2024-24783 CVE-2024-24784 CVE-2024-24785 CVE-2024-24786	RedHat	Medium	Run Once Duration Override Operator for Red Hat OpenShift 1.1.1 for RHEL 9	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:1616
	05	CVE-2024-2199 CVE-2024-3657	RedHat	High	389-ds security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4235
	06	CVE-2024-24789 CVE-2024-24790	RedHat	Medium	go-toolset security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4237
2-Aug	07	CVE-2015-7501 CVE-2022-23457 CVE-2022-42920 CVE-2015-0226 CVE-2015-6420 CVE-2021-40690 CVE-2022-40149 CVE-2022-40150 CVE-2022-40152 CVE-2022-45685 CVE-2022-45693 CVE-2023-1436 CVE-2023-3635 CVE-2022-24329 CVE-2023-47100	HPE	Critical	HPESBNW04558 rev.2 - HPE Telecommunication Management Information Platform (vTeMIP) , Multiple Vulnerabilities	Updates are available please see below reference link: https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04558en_us&docLocale=en_US
	08	CVE-2024-1062 CVE-2024-2199 CVE-2024-3657	RedHat	High	redhat-ds:11 security and bug fix update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4209

	09	CVE-2024-2199 CVE-2024-3657	RedHat	High	redhat-ds:11 security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4210
	10	CVE-2024-26583 CVE-2024-26584 CVE-2024-26585 CVE-2024-26656 CVE-2024-26675 CVE-2024-26735 CVE-2024-26759 CVE-2024-26801 CVE-2024-26804 CVE-2024-26826 CVE-2024-26859 CVE-2024-26906 CVE-2024-26907 CVE-2024-26974 CVE-2024-26982 CVE-2024-27397 CVE-2024-27410 CVE-2024-35789 CVE-2024-35835 CVE-2024-35838 CVE-2024-35845 CVE-2024-35852 CVE-2024-35853 CVE-2024-35854 CVE-2024-35855 CVE-2024-35888 CVE-2024-35890 CVE-2024-35958 CVE-2024-35959 CVE-2024-35960 CVE-2024-36004 CVE-2024-36007	RedHat	High	kernel security and bug fix update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4211
5-Aug	11	CVE-2022-48651 CVE-2024-26610 CVE-2024-26828 CVE-2024-26852 CVE-2024-26923 CVE-2024-27398 CVE-2024-35950	SUSU	High	Security update for the Linux Kernel RT (Live Patch 13 for SLE 15 SP5)	Updates are available please see below reference link: https://www.suse.com/support/update/announcement/2024/suse-su-20242725-1/
	12	CVE-2021-47383 CVE-2023-1829 CVE-2024-26828 CVE-2024-26923 CVE-2024-27398 CVE-2024-35950	SUSU	High	Security update for the Linux Kernel (Live Patch 48 for SLE 15 SP2)	Updates are available please see below reference link: https://www.suse.com/support/update/announcement/2024/suse-su-20242759-1/
	13	CVE-2021-46955 CVE-2021-47383 CVE-2022-48651 CVE-2023-1829 CVE-2024-23307 CVE-2024-26828 CVE-2024-26852 CVE-2024-26923 CVE-2024-27398 CVE-2024-35950	SUSU	High	Security update for the Linux Kernel (Live Patch 47 for SLE 15 SP2)	Updates are available please see below reference link: https://www.suse.com/support/update/announcement/2024/suse-su-20242758-1/

	14	CVE-2022-48651 CVE-2023-52502 CVE-2023-6546 CVE-2024-23307 CVE-2024-26610 CVE-2024-26828 CVE-2024-26852 CVE-2024-26923 CVE-2024-26930 CVE-2024-27398 CVE-2024-35950	SUSU	High	Security update for the Linux Kernel RT (Live Patch 11 for SLE 15 SP5)	Updates are available please see below reference link: https://www.suse.com/support/update/announcement/2024/suse-su-20242751-1/
	15	CVE-2020-9484 CVE-2021-41079 CVE-2022-29885 CVE-2022-23181 CVE-2021-25122	Ubuntu	Medium	Tomcat vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6943-1
	16	CVE-2024-1975 CVE-2024-1737	Ubuntu	Medium	Bind vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6909-2
	17	CVE-2024-41990 CVE-2024-42005 CVE-2024-41989 CVE-2024-41991	Ubuntu	Medium	Django vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6946-1
6-Aug	18	CVE-2024-6387	HPE	High	HPE Athonet Unauthenticated Remote Code Execution (RCE) Vulnerability in OpenSSH's Server	Updates are available please see below reference link: https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04674en_us&docLocale=en_US
	19	CVE-2024-21131 CVE-2024-21138 CVE-2024-21140 CVE-2024-21144 CVE-2024-21145 CVE-2024-21147	SUSU	High	Security update for java-1_8_0-openjdk	Updates are available please see below reference link: https://www.suse.com/support/update/announcement/2024/suse-su-20242766-1/
	20	CVE-2024-31080 CVE-2024-31081 CVE-2024-31083	SUSU	Medium	Security update for dri3proto, presentproto, wayland-protocols, xwayland	Updates are available please see below reference link: https://www.suse.com/support/update/announcement/2024/suse-su-20242776-1/
	21	CVE-2024-5290	Ubuntu	Medium	wpa_supplicant and hostapd vulnerability	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6945-1
	22	CVE-2024-6600 CVE-2024-6601 CVE-2024-6602 CVE-2024-6603 CVE-2024-6604	SUSU	High	Security update for MozillaThunderbird	Updates are available please see below reference link: https://www.suse.com/support/update/announcement/2024/suse-su-20242790-1/
	23	CVE-2024-21131 CVE-2024-21138 CVE-2024-21140 CVE-2024-21145 CVE-2024-21147 CVE-2024-21144	Oracle	Medium	java-11-openjdk security update	Updates are available please see below reference link: https://linux.oracle.com/errata/ELSA-2024-4564.html

	24	CVE-2024-38811	VMWare	High	VMware Fusion update addresses a code execution vulnerability	Updates are available please see below reference link: https://support.broadcom.com/web/ecx/security-advisory
7-Aug	25	CVE-2018-20843 CVE-2019-15903 CVE-2021-46143 CVE-2022-22825 CVE-2022-23990 CVE-2020-24977 CVE-2021-3517 CVE-2021-3518 CVE-2021-3537 CVE-2021-3541 CVE-2022-40304 CVE-2022-40303 CVE-2023-28484 CVE-2023-29469 CVE-2024-5462 CVE-2024-5461	HPE	High	HPE Fibre Channel and SAN Switches with Brocade Fabric OS (FOS)	Updates are available please see below reference link: https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbst04679en_us&docLocale=en_US
	26	CVE-2021-47400 CVE-2023-52626 CVE-2023-52667 CVE-2024-26801 CVE-2024-26974 CVE-2024-27393 CVE-2024-35870 CVE-2024-35960	RedHat	Medium	kernel security and bug fix update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4349
	27	CVE-2022-48651 CVE-2023-52502 CVE-2023-6546 CVE-2024-23307 CVE-2024-26610 CVE-2024-26766 CVE-2024-26828 CVE-2024-26852 CVE-2024-26923 CVE-2024-26930 CVE-2024-27398 CVE-2024-35950	SUSU	High	Security update for the Linux Kernel (Live Patch 25 for SLE 15 SP4)	Updates are available please see below reference link: https://www.suse.com/support/update/announcement/2024/suse-su-20242825-1/
8-Aug	28	CVE-2024-37371 CVE-2024-37370	Ubuntu	Medium	Kerberos vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6947-1
	29	CVE-2020-16846 CVE-2020-25592 CVE-2020-28972 CVE-2020-28243 CVE-2021-25281 CVE-2021-3148 CVE-2020-17490 CVE-2020-35662 CVE-2021-3197 CVE-2021-25282 CVE-2021-25284 CVE-2021-25283	Ubuntu	Medium	Salt vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6948-1

	30	CVE-2020-26555 CVE-2021-46909 CVE-2021-46972 CVE-2021-47069 CVE-2021-47073 CVE-2021-47236 CVE-2021-47310 CVE-2021-47311 CVE-2021-47353 CVE-2021-47356 CVE-2021-47456 CVE-2021-47495 CVE-2023-5090 CVE-2023-52464 CVE-2023-52560 CVE-2023-52615 CVE-2023-52626 CVE-2023-52667 CVE-2023-52700 CVE-2023-52703 CVE-2023-52781 CVE-2023-52813 CVE-2023-52835 CVE-2023-52877 CVE-2023-52878 CVE-2023-52881 CVE-2024-26583 CVE-2024-26584 CVE-2024-26585 CVE-2024-26656 CVE-2024-26675 CVE-2024-26735 CVE-2024-26759 CVE-2024-26801 CVE-2024-26804 CVE-2024-26826 CVE-2024-26859 CVE-2024-26906 CVE-2024-26907 CVE-2024-26974 CVE-2024-26982 CVE-2024-27397 CVE-2024-27410 CVE-2024-35789 CVE-2024-35835 CVE-2024-35838 CVE-2024-35845 CVE-2024-35852 CVE-2024-35853 CVE-2024-35854 CVE-2024-35855 CVE-2024-35888 CVE-2024-35890 CVE-2024-35958 CVE-2024-35959 CVE-2024-35960 CVE-2024-36004 CVE-2024-36007	RedHat	High	kernel-rt security and bug fix update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4352

9-Aug	31	CVE-2024-3653 CVE-2024-5971 CVE-2024-27316 CVE-2024-29025 CVE-2024-29857 CVE-2024-30171 CVE-2024-30172	RedHat	High	Red Hat JBoss Enterprise Application Platform 7.4.18 Security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5147
	32	CVE-2024-3653 CVE-2024-5971 CVE-2024-27316 CVE-2024-29025 CVE-2024-29857 CVE-2024-30171 CVE-2024-30172	RedHat	High	Red Hat JBoss Enterprise Application Platform 7.4.18 Security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5143
	33	CVE-2024-3653 CVE-2024-5971 CVE-2024-27316 CVE-2024-29025 CVE-2024-29857 CVE-2024-30171 CVE-2024-30172	RedHat	High	Red Hat JBoss Enterprise Application Platform 7.4.18 Security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5144
	34	CVE-2024-26828 CVE-2024-26852 CVE-2024-26923 CVE-2024-26930 CVE-2024-27398 CVE-2024-35950	SUSU	High	Security update for the Linux Kernel (Live Patch 26 for SLE 15 SP4)	Updates are available please see below reference link: https://www.suse.com/support/update/announcement/2024/suse-su-20242841-1/
	35	CVE-2022-48651 CVE-2023-52502 CVE-2023-6546 CVE-2024-23307 CVE-2024-26610 CVE-2024-26766 CVE-2024-26828 CVE-2024-26852 CVE-2024-26923 CVE-2024-26930 CVE-2024-27398 CVE-2024-35950	SUSU	High	Security update for the Linux Kernel (Live Patch 24 for SLE 15 SP4)	Updates are available please see below reference link: https://www.suse.com/support/update/announcement/2024/suse-su-20242840-1/
12-Aug	36	CVE-2024-1737 CVE-2024-1975 CVE-2024-4076	RedHat	High	bind and bind-dyndb-ldap security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5194
	37	CVE-2024-6104 CVE-2024-37298	RedHat	High	container-tools:rhel8 security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5231
	38	CVE-2024-5953 CVE-2024-6237	RedHat	Medium	389-ds-base security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5192
	39	CVE-2023-45935 CVE-2024-39936	SUSU	High	Security update for libqt5-qtbase	Updates are available please see below reference link: https://www.suse.com/support/

						update/announcement/2024/suse-su-20242883-1/
	40	CVE-2024-6600 CVE-2024-6601 CVE-2024-6602 CVE-2024-6603 CVE-2024-6604 CVE-2024-6605 CVE-2024-6606 CVE-2024-6607 CVE-2024-6608 CVE-2024-6609 CVE-2024-6610 CVE-2024-6611 CVE-2024-6612 CVE-2024-6613 CVE-2024-6614 CVE-2024-6615 CVE-2024-7518 CVE-2024-7519 CVE-2024-7520 CVE-2024-7521 CVE-2024-7522 CVE-2024-7524 CVE-2024-7525 CVE-2024-7526 CVE-2024-7527 CVE-2024-7528 CVE-2024-7529 CVE-2024-7531	SUSU	High	Security update for MozillaFirefox	Updates are available please see below reference link: https://www.suse.com/support/update/announcement/2024/suse-su-20242876-1/
	41	CVE-2024-33861 CVE-2024-39936	SUSU	High	Security update for qt6-base	Updates are available please see below reference link: https://www.suse.com/support/update/announcement/2024/suse-su-20242875-1/
	42	CVE-2024-41671 CVE-2024-41810	SUSU	High	Security update for python-Twisted	Updates are available please see below reference link: https://www.suse.com/support/update/announcement/2024/suse-su-20242880-1/
13-Aug	43	CVE-2017-8834 CVE-2020-12825 CVE-2017-7960 CVE-2017-8871	Ubuntu	Medium	Libcroco vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6958-1
	44	CVE-2023-6693 CVE-2023-6683 CVE-2024-24474	Ubuntu	Medium	QEMU vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6954-1
	45	CVE-2022-48827 CVE-2022-48828 CVE-2022-48829 CVE-2024-36005 CVE-2024-36971 CVE-2024-39502	RedHat	High	kernel-rt security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5282

	46	CVE-2021-47311 CVE-2021-47385 CVE-2021-47566 CVE-2022-48637 CVE-2022-48827 CVE-2022-48828 CVE-2022-48829 CVE-2023-52439 CVE-2023-52448 CVE-2023-52881 CVE-2023-52885 CVE-2024-21823 CVE-2024-35852 CVE-2024-36017 CVE-2024-36971 CVE-2024-39502 CVE-2024-41090 CVE-2024-41091	RedHat	High	kernel security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5281
	47	CVE-2024-38473 CVE-2024-38474 CVE-2024-38475 CVE-2024-38476 CVE-2024-38477 CVE-2024-39573	RedHat	High	Red Hat JBoss Core Services Apache HTTP Server 2.4.57 SP5 security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5239
	48	CVE-2024-38473 CVE-2024-38474 CVE-2024-38475 CVE-2024-38476 CVE-2024-38477 CVE-2024-39573	RedHat	High	Red Hat JBoss Core Services Apache HTTP Server 2.4.57 SP5 security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5240
	49	CVE-2023-45918 CVE-2024-6104 CVE-2024-34064 CVE-2024-34069 CVE-2024-38473 CVE-2024-39573	RedHat	High	OpenShift Container Platform 4.16.7 bug fix and security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5107

14-Aug	50	CVE-2021-47383 CVE-2023-52448 CVE-2023-52651 CVE-2023-52771 CVE-2023-52864 CVE-2024-21823 CVE-2024-26855 CVE-2024-26897 CVE-2024-27046 CVE-2024-27052 CVE-2024-35789 CVE-2024-35845 CVE-2024-35852 CVE-2024-35907 CVE-2024-35937 CVE-2024-36922 CVE-2024-36941 CVE-2024-36971 CVE-2024-38538 CVE-2024-38555 CVE-2024-38556 CVE-2024-38586 CVE-2024-38627	RedHat	High	kernel-rt security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5365
	51	CVE-2021-47383 CVE-2023-52448 CVE-2023-52651 CVE-2023-52771 CVE-2023-52864 CVE-2024-21823 CVE-2024-26855 CVE-2024-26897 CVE-2024-27046 CVE-2024-27052 CVE-2024-35789 CVE-2024-35845 CVE-2024-35852 CVE-2024-35907 CVE-2024-35937 CVE-2024-36922 CVE-2024-36941 CVE-2024-36971 CVE-2024-38538 CVE-2024-38555 CVE-2024-38556 CVE-2024-38586 CVE-2024-38627	RedHat	High	kernel security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5364
	52	CVE-2023-42363 CVE-2022-48174 CVE-2023-42364 CVE-2023-42365	Ubuntu	Medium	BusyBox vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6961-1
	53	CVE-2024-2199 CVE-2024-3657 CVE-2024-5953	SUSU	High	Security update for 389-ds	Updates are available please see below reference link: https://www.suse.com/support/update/announcement/2024/suse-su-20242910-1/

	54	CVE-2024-40776 CVE-2024-40779 CVE-2024-40780 CVE-2024-40782	SUSU	High	Security update for webkit2gtk3	Updates are available please see below reference link: https://www.suse.com/support/update/announcement/2024/suse-su-20242905-1/
16-Aug	55	CVE-2024-1737 CVE-2024-1975 CVE-2024-4076	RedHat	High	bind9.16 security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5418
	56	CVE-2024-7519 CVE-2024-7521 CVE-2024-7526 CVE-2024-7527 CVE-2024-7529 CVE-2024-7518 CVE-2024-7522 CVE-2024-7525 CVE-2024-7520 CVE-2024-7524 CVE-2024-7528	Oracle	High	firefox security update	Updates are available please see below reference link: https://linux.oracle.com/errata/ELSA-2024-5391.html
	57	CVE-2024-1975 CVE-2024-1737 CVE-2024-4076	Oracle	High	bind9.16 security update	Updates are available please see below reference link: https://linux.oracle.com/errata/ELSA-2024-5390.html
	58	CVE-2024-7519 CVE-2024-7527 CVE-2024-7520 CVE-2024-7522 CVE-2024-7528 CVE-2024-7518 CVE-2024-7521 CVE-2024-7525 CVE-2024-7529 CVE-2024-7526	Oracle	High	thunderbird security update	Updates are available please see below reference link: https://linux.oracle.com/errata/ELSA-2024-5392.html
	59	CVE-2024-7528 CVE-2024-7520 CVE-2024-7527 CVE-2024-7522 CVE-2024-7529 CVE-2024-7519 CVE-2024-7521 CVE-2024-7526 CVE-2024-7525 CVE-2024-7518	Oracle	High	thunderbird security update	Updates are available please see below reference link: https://linux.oracle.com/errata/ELSA-2024-5402.html
20-Aug	60	CVE-2024-1737 CVE-2024-1975 CVE-2024-4076	RedHat	High	bind9.16 security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5525

	61	CVE-2024-29894 CVE-2024-31460 CVE-2024-31458 CVE-2024-31443 CVE-2024-31444 CVE-2024-25641 CVE-2024-34340 CVE-2024-31445 CVE-2024-31459	Ubuntu	Medium	Cacti vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6969-1
	62	CVE-2023-42667 CVE-2024-24853 CVE-2024-25939 CVE-2024-24980 CVE-2023-49141	Ubuntu	Medium	Intel Microcode vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6967-1
	63	CVE-2024-38155	Microsoft	Medium	Security Center Broker Information Disclosure Vulnerability	Updates are available please see below reference link: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38155
	64	CVE-2024-38210	Microsoft	High	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	Updates are available please see below reference link: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38210
	65	CVE-2024-38208	Microsoft	Medium	Microsoft Edge for Android Spoofing Vulnerability	Updates are available please see below reference link: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38208
	66	CVE-2024-41879	Microsoft	Medium	Adobe Systems Incorporated: CVE-2024-41879 Adobe PDF Viewer Remote Code Execution Vulnerability	Updates are available please see below reference link: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-41879
	67	CVE-2024-38209	Microsoft	High	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	Updates are available please see below reference link: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38209
	68	CVE-2024-38186	Microsoft	High	Windows Kernel-Mode Driver Elevation of Privilege Vulnerability	Updates are available please see below reference link: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38186
	69	CVE-2024-38155	Microsoft	High	Security Center Broker Information Disclosure Vulnerability	Updates are available please see below reference link: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38155
	70	CVE-2024-38146	Microsoft	High	Windows Layer-2 Bridge Network Driver Denial of Service Vulnerability	Updates are available please see below reference link: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38146

	71	CVE-2024-38143	Microsoft	High	Windows WLAN AutoConfig Service Elevation of Privilege Vulnerability	Updates are available please see below reference link: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38143
	72	CVE-2024-38122	Microsoft	High	Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability	Updates are available please see below reference link: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38122
	73	CVE-2024-37968	Microsoft	High	Windows DNS Spoofing Vulnerability	Updates are available please see below reference link: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37968
	74	CVE-2024-7518 CVE-2024-7529 CVE-2024-7521 CVE-2024-7524 CVE-2024-7525 CVE-2024-7530 CVE-2024-7522 CVE-2024-7520 CVE-2024-7527 CVE-2024-7531 CVE-2024-7519 CVE-2024-7528 CVE-2024-7526	Ubuntu	Medium	Firefox vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6966-1
21-Aug	75	CVE-2024-37370 CVE-2024-37371	RedHat	Medium	krb5 security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5625
	76	CVE-2023-45290 CVE-2024-24790 CVE-2024-37298	RedHat	Medium	OpenShift Container Platform 4.12.63 packages and security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5202
	77	CVE-2023-45290 CVE-2023-48795 CVE-2024-5037 CVE-2024-6104 CVE-2024-6345 CVE-2024-6409 CVE-2024-24790 CVE-2024-34064 CVE-2024-35235 CVE-2024-36971 CVE-2024-37298 CVE-2024-37891 CVE-2024-38428 CVE-2024-38473 CVE-2024-39331 CVE-2024-39573	RedHat	High	OpenShift Container Platform 4.12.63 bug fix and security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5200
	78	CVE-2024-24788 CVE-2024-24789 CVE-2024-24790 CVE-2024-24791 CVE-2024-37370	RedHat	Medium	Red Hat build of Cryostat security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5537

		CVE-2024-37371 CVE-2024-37891				
	79	CVE-2024-7518 CVE-2024-7519 CVE-2024-7520 CVE-2024-7521 CVE-2024-7522 CVE-2024-7525 CVE-2024-7526 CVE-2024-7527 CVE-2024-7528 CVE-2024-7529	RedHat	High	thunderbird security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5528
22-Aug	80	CVE-2023-52463 CVE-2023-52735 CVE-2024-26853 CVE-2024-36000 CVE-2024-36883 CVE-2024-38608 CVE-2024-40995 CVE-2024-41076 CVE-2024-41090 CVE-2024-41091 CVE-2024-42107	RedHat	High	kernel security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5672
	81	CVE-2023-52463 CVE-2023-52735 CVE-2024-26853 CVE-2024-36000 CVE-2024-36883 CVE-2024-38608 CVE-2024-40995 CVE-2024-41076 CVE-2024-41090 CVE-2024-41091 CVE-2024-42107	RedHat	High	kernel-rt security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5673
	82	CVE-2021-46939 CVE-2021-47018 CVE-2021-47257 CVE-2021-47284 CVE-2021-47304 CVE-2021-47373 CVE-2021-47408 CVE-2021-47461 CVE-2021-47468 CVE-2021-47491 CVE-2021-47548 CVE-2021-47579 CVE-2021-47624 CVE-2022-48632 CVE-2022-48743 CVE-2022-48747 CVE-2022-48757 CVE-2023-28746 CVE-2023-48795 CVE-2023-52451 CVE-2023-52463	RedHat	Medium	OpenShift Container Platform 4.15.28 packages and security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5438

		CVE-2023-52469 CVE-2023-52471 CVE-2023-52486 CVE-2023-52530 CVE-2023-52619 CVE-2023-52622 CVE-2023-52623 CVE-2023-52648 CVE-2023-52653 CVE-2023-52658 CVE-2023-52662 CVE-2023-52679 CVE-2023-52707 CVE-2023-52730 CVE-2023-52756 CVE-2023-52762 CVE-2023-52764 CVE-2023-52775 CVE-2023-52777 CVE-2023-52784 CVE-2023-52791 CVE-2023-52796 CVE-2023-52803 CVE-2023-52811 CVE-2023-52832 CVE-2023-52834 CVE-2023-52845 CVE-2023-52847 CVE-2023-52864 CVE-2024-2201 CVE-2024-6345 CVE-2024-21823 CVE-2024-25739 CVE-2024-26586 CVE-2024-26614 CVE-2024-26640 CVE-2024-26660 CVE-2024-26669 CVE-2024-26686 CVE-2024-26698 CVE-2024-26704 CVE-2024-26733 CVE-2024-26740 CVE-2024-26772 CVE-2024-26773 CVE-2024-26802 CVE-2024-26810 CVE-2024-26837 CVE-2024-26840 CVE-2024-26843 CVE-2024-26852 CVE-2024-26853 CVE-2024-26870 CVE-2024-26878 CVE-2024-26908 CVE-2024-26921 CVE-2024-26925 CVE-2024-26940 CVE-2024-26958				

		CVE-2024-26960 CVE-2024-26961 CVE-2024-27010 CVE-2024-27011 CVE-2024-27019 CVE-2024-27020 CVE-2024-27025 CVE-2024-27065 CVE-2024-27388 CVE-2024-27395 CVE-2024-27434 CVE-2024-31076 CVE-2024-33621 CVE-2024-35790 CVE-2024-35801 CVE-2024-35807 CVE-2024-35810 CVE-2024-35814 CVE-2024-35823 CVE-2024-35824 CVE-2024-35847 CVE-2024-35876 CVE-2024-35893 CVE-2024-35896 CVE-2024-35897 CVE-2024-35899 CVE-2024-35900 CVE-2024-35910 CVE-2024-35912 CVE-2024-35924 CVE-2024-35925 CVE-2024-35930 CVE-2024-35937 CVE-2024-35938 CVE-2024-35946 CVE-2024-35947 CVE-2024-35952 CVE-2024-36000 CVE-2024-36005 CVE-2024-36006 CVE-2024-36010 CVE-2024-36016 CVE-2024-36017 CVE-2024-36020 CVE-2024-36025 CVE-2024-36270 CVE-2024-36286 CVE-2024-36489 CVE-2024-36886 CVE-2024-36889 CVE-2024-36896 CVE-2024-36904 CVE-2024-36905 CVE-2024-36917 CVE-2024-36921 CVE-2024-36927 CVE-2024-36929 CVE-2024-36933 CVE-2024-36940				

		CVE-2024-36941 CVE-2024-36945 CVE-2024-36950 CVE-2024-36954 CVE-2024-36960 CVE-2024-36971 CVE-2024-36978 CVE-2024-36979 CVE-2024-38538 CVE-2024-38555 CVE-2024-38573 CVE-2024-38575 CVE-2024-38596 CVE-2024-38598 CVE-2024-38615 CVE-2024-38627 CVE-2024-39276 CVE-2024-39472 CVE-2024-39476 CVE-2024-39487 CVE-2024-39502 CVE-2024-40927 CVE-2024-40974				
23-Aug	83	CVE-2024-1062 CVE-2024-2199 CVE-2024-3657 CVE-2024-5953	RedHat	High	389-ds:1.4 security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5690
	84	CVE-2021-3974 CVE-2021-3973 CVE-2021-4019 CVE-2021-3984 CVE-2021-4069	Ubuntu	Medium	Vim vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6965-1
	85	CVE-2024-39292 CVE-2023-52644 CVE-2023-52470 CVE-2024-26654 CVE-2024-26903 CVE-2024-26600 CVE-2023-52629 CVE-2024-26687 CVE-2024-39484 CVE-2024-36940 CVE-2024-35835 CVE-2023-52806 CVE-2024-26679 CVE-2024-36901 CVE-2024-35955 CVE-2023-52760 CVE-2024-24860 CVE-2024-22099	Ubuntu	Medium	Linux kernel (AWS) vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6972-2

	86	CVE-2021-21342 CVE-2021-21344 CVE-2021-21349 CVE-2021-21346 CVE-2021-21347 CVE-2021-21350 CVE-2021-21345 CVE-2021-21343 CVE-2016-3674 CVE-2020-26258 CVE-2021-21348 CVE-2020-26217 CVE-2020-26259 CVE-2021-21341 CVE-2021-21351	Ubuntu	Medium	XStream vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6978-1
	87	CVE-2018-18025 CVE-2018-17966 CVE-2018-16412 CVE-2018-16413 CVE-2018-18024 CVE-2018-18016 CVE-2018-20467 CVE-2017-12806 CVE-2017-12805 CVE-2017-13144	Ubuntu	Medium	ImageMagick vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6980-1
26-Aug	88	CVE-2024-22018 CVE-2024-22020 CVE-2024-36137	RedHat	Medium	nodejs:20 security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5815
	89	CVE-2024-22018 CVE-2024-22020 CVE-2024-28863 CVE-2024-36137	RedHat	Medium	nodejs:20 security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5814
	90	CVE-2024-1737 CVE-2024-1975 CVE-2024-4076	RedHat	High	bind and bind-dyndb-ldap security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5813
	91	CVE-2024-31145 CVE-2024-31146	SUSU	High	Security update for xen	Updates are available please see below reference link: https://www.suse.com/support/update/announcement/2024/suse-su-20243010-1/
	92	CVE-2024-39484 CVE-2024-26921 CVE-2023-52760 CVE-2024-26680 CVE-2024-36901 CVE-2024-39292 CVE-2024-26830 CVE-2023-52629	Ubuntu	Medium	Linux kernel (Oracle) vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6974-2

	93	CVE-2024-39484 CVE-2023-52806 CVE-2023-52470 CVE-2023-52644 CVE-2024-24860 CVE-2024-26903 CVE-2024-36940 CVE-2024-26654 CVE-2024-26679 CVE-2024-22099 CVE-2024-35955 CVE-2024-39292 CVE-2024-26687 CVE-2024-26600 CVE-2023-52760 CVE-2024-35835 CVE-2023-52629 CVE-2024-36901	Ubuntu	Medium	Linux kernel (Azure) vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6972-3
	94	CVE-2024-39484 CVE-2024-24860 CVE-2024-26921 CVE-2023-52760 CVE-2024-36901 CVE-2024-26830 CVE-2021-46926 CVE-2024-26929 CVE-2023-52629	Ubuntu	Medium	Linux kernel (Azure) vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6973-2
27-Aug	95	CVE-2024-2004 CVE-2024-2379 CVE-2024-2398 CVE-2024-2466 CVE-2024-6197 CVE-2024-6874 CVE-2024-40725 CVE-2024-40898 CVE-2024-39884 CVE-2024-39573 CVE-2024-38477 CVE-2024-38476 CVE-2024-38475 CVE-2024-38474 CVE-2024-38473 CVE-2024-38472 CVE-2024-36387	Tenable	Critical	Stand-alone Security Patch Available for Tenable Security Center versions 6.2.1, 6.3.0 and 6.4.0: SC-202408.1	Updates are available please see below reference link: https://www.tenable.com/security/tns-2024-13
	96	CVE-2024-1737 CVE-2024-1975 CVE-2024-4076	RedHat	High	bind and bind-dyndb-ldap security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5907
	97	CVE-2024-1737 CVE-2024-1975	RedHat	High	bind security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5908
	98	CVE-2024-21096	SUSU	Medium	Security update for mariadb	Updates are available please see below reference link: https://www.suse.com/support/update/announcement/2024/suse-su-20243018-1/

	99	CVE-2024-5535	SUSU	Medium	Security update for openssl-3	Updates are available please see below reference link: https://www.suse.com/support/update/announcement/2024/suse-su-20243019-1/
	100	CVE-2024-35955 CVE-2024-39484 CVE-2024-24860 CVE-2024-26654 CVE-2024-26679 CVE-2023-52760 CVE-2023-52644 CVE-2024-36901 CVE-2024-26903 CVE-2024-36940 CVE-2024-39292 CVE-2023-52470 CVE-2024-26687 CVE-2024-22099 CVE-2023-52806 CVE-2024-35835 CVE-2024-26600 CVE-2023-52629	Ubuntu	Medium	Linux kernel (Oracle) vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6972-4
	101	CVE-2020-13671 CVE-2020-28949 CVE-2020-28948	Ubuntu	High	Drupal vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6981-1
28-Aug	102	CVE-2023-52771 CVE-2023-52880 CVE-2024-26581 CVE-2024-26668 CVE-2024-26810 CVE-2024-26855 CVE-2024-26908 CVE-2024-26925 CVE-2024-27016 CVE-2024-27019 CVE-2024-27020 CVE-2024-27415 CVE-2024-35839 CVE-2024-35896 CVE-2024-35897 CVE-2024-35898 CVE-2024-35962 CVE-2024-36003 CVE-2024-36025 CVE-2024-38538 CVE-2024-38540 CVE-2024-38544 CVE-2024-38579 CVE-2024-38608 CVE-2024-39476 CVE-2024-40905 CVE-2024-40911 CVE-2024-40912 CVE-2024-40914 CVE-2024-40929 CVE-2024-40939 CVE-2024-40941	RedHat	High	kernel security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5928

		CVE-2024-40957 CVE-2024-40978 CVE-2024-40983 CVE-2024-41041 CVE-2024-41076 CVE-2024-41090 CVE-2024-41091 CVE-2024-42110 CVE-2024-42152				
	103	CVE-2024-4317 CVE-2024-7348	RedHat	High	postgresql:16 security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5929
	104	CVE-2024-4317 CVE-2024-7349	Oracle	High	postgresql:16 security update	Updates are available please see below reference link: https://linux.oracle.com/errata/ELSA-2024-5929.html
	105	CVE-2021-47383 CVE-2023-52448 CVE-2023-52651 CVE-2023-52771 CVE-2023-52864 CVE-2024-1737 CVE-2024-1975 CVE-2024-3727 CVE-2024-6345 CVE-2024-21823 CVE-2024-26855 CVE-2024-26897 CVE-2024-27046 CVE-2024-27052 CVE-2024-35789 CVE-2024-35845 CVE-2024-35852 CVE-2024-35907 CVE-2024-35937 CVE-2024-36922 CVE-2024-36941 CVE-2024-36971 CVE-2024-37370 CVE-2024-37371 CVE-2024-37891 CVE-2024-38428 CVE-2024-38538 CVE-2024-38555 CVE-2024-38556 CVE-2024-38586 CVE-2024-38627	RedHat	Low	OpenShift Virtualization 4.15.5 Images	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5951
29-Aug	106	CVE-2021-47069 CVE-2021-47356 CVE-2021-47468 CVE-2022-48793 CVE-2022-48799 CVE-2023-6597 CVE-2023-45290 CVE-2023-52434 CVE-2023-52463 CVE-2023-52610	RedHat	Medium	OpenShift Container Platform 4.12.64 security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5808

		CVE-2023-52735 CVE-2023-52864 CVE-2024-6104 CVE-2024-24788 CVE-2024-24790 CVE-2024-26853 CVE-2024-34064 CVE-2024-34069 CVE-2024-35845 CVE-2024-36000 CVE-2024-36016 CVE-2024-36883 CVE-2024-36904 CVE-2024-36941 CVE-2024-37370 CVE-2024-37371 CVE-2024-38570 CVE-2024-38608 CVE-2024-40995 CVE-2024-41076 CVE-2024-41090 CVE-2024-41091 CVE-2024-42107				
	107	CVE-2023-31315	RedHat	High	linux-firmware security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:5978
	108	CVE-2024-4032 CVE-2024-8088 CVE-2024-6923 CVE-2024-6345	Oracle	Medium	python39:3.9 and python39-devel:3.9 security update	Updates are available please see below reference link: https://linux.oracle.com/errata/ELSA-2024-5962.html

SOME ZERO-DAY VULNERABILITITIES OF THE MONTH

Sl. No	Title	Vendor	Severity	Summary
01	Red Hat Certificate System security and bug fix update	RedHat	High	Red Hat Certificate System is a complete implementation of an enterprise software system designed to manage enterprise public key infrastructure (PKI) deployments. Bug fix(es): Coolkey Hardcoded RSA Max Key Size (BZ#2047831) Add Secure Channel Support for AES-256 Keys (BZ#2121463) TPS missing Host header field in HTTP/1.1 request message (BZ#2177785) Add AES support for TMS server-side keygen on latest HSM / FIPS environment (BZ#2180920) Make key wrapping algorithm configurable between AES-KWP and AES-CBC (BZ#2233158) pkidestroy log keeps HSM token password (BZ#2253682) Add Support for Symmetric Key Rollover (BZ#2265180) Users of Red Hat Certificate System are advised to install these updated packages.
02	Security update for ca-certificates-mozilla	SUSU	High	This update for ca-certificates-mozilla fixes the following issues: Updated to 2.68 state of Mozilla SSL root CAs (bsc#1227525) Added: FIRMAPROFESIONAL CA ROOT-A WEB Distrust: GLOBALTRUST 2020 Updated to 2.66 state of Mozilla SSL root CAs (bsc#1220356) Added: CommScope Public Trust ECC Root-01 CommScope Public Trust ECC Root-02 CommScope Public Trust RSA Root-01 CommScope Public Trust RSA Root-02 D-Trust SBR Root CA 1 2022 D-Trust SBR Root CA 2 2022 Telekom Security SMIME ECC Root 2021 Telekom Security SMIME RSA Root 2023 Telekom Security TLS ECC Root 2020 Telekom Security TLS RSA Root 2023 TrustAsia Global Root CA G3 TrustAsia Global Root CA G4 Removed: Autoridad de Certificacion Firmaprofesional CIF A62634068 Chambers of Commerce Root - 2008 Global Chambersign Root - 2008

				Security Communication Root CA Symantec Class 1 Public Primary Certification Authority - G6 Symantec Class 2 Public Primary Certification Authority - G6 TrustCor ECA-1 TrustCor RootCert CA-1 TrustCor RootCert CA-2 VeriSign Class 1 Public Primary Certification Authority - G3 VeriSign Class 2 Public Primary Certification Authority - G3

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