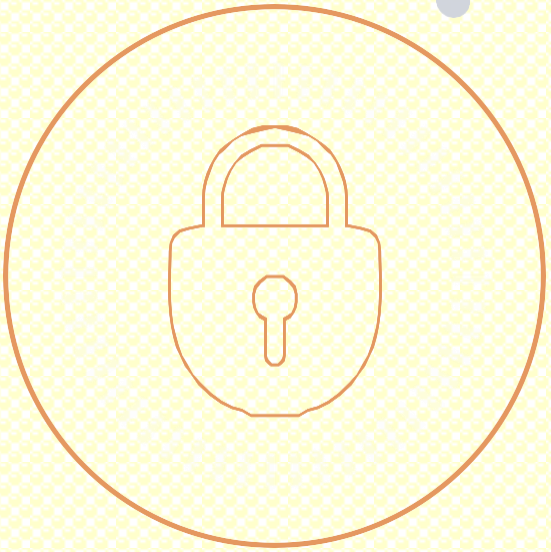
SECURITY INTELLIGENCE ADVISORY



01st July 2024 – 31st July 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.

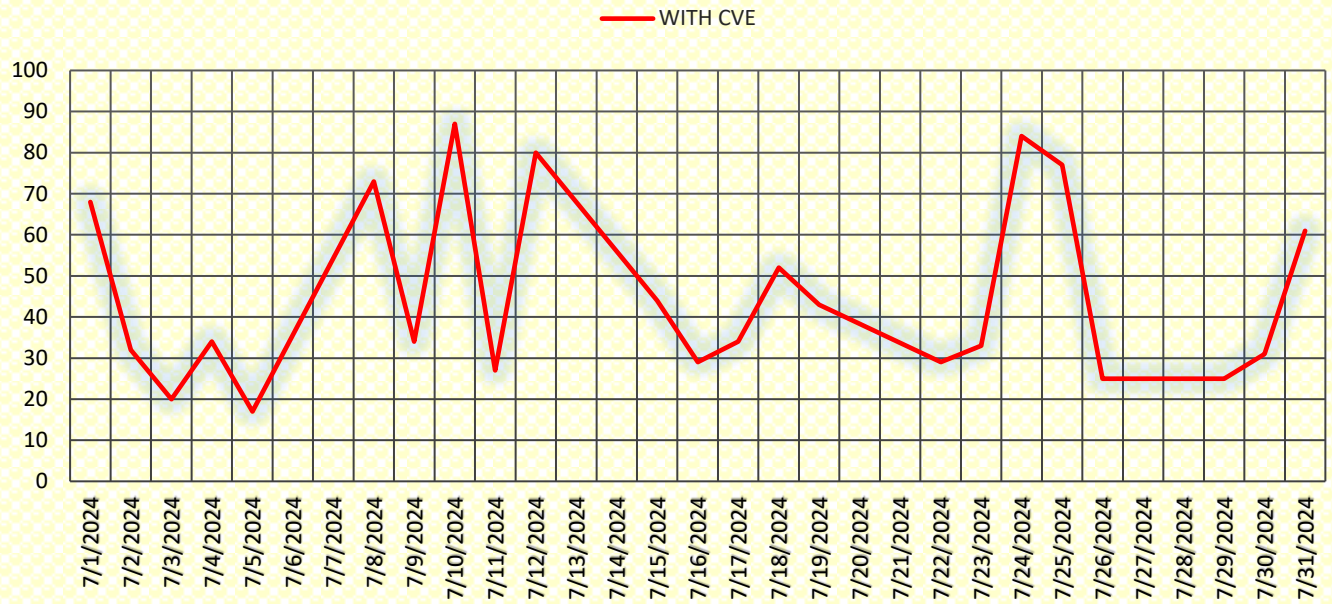
One effective way to stay on top of these vulnerabilities is by conducting regular vulnerability assessments. These periodic assessments cover your entire IT infrastructure and help you identify new threats that may have emerged. This proactive practice enables you to stay abreast of the current state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

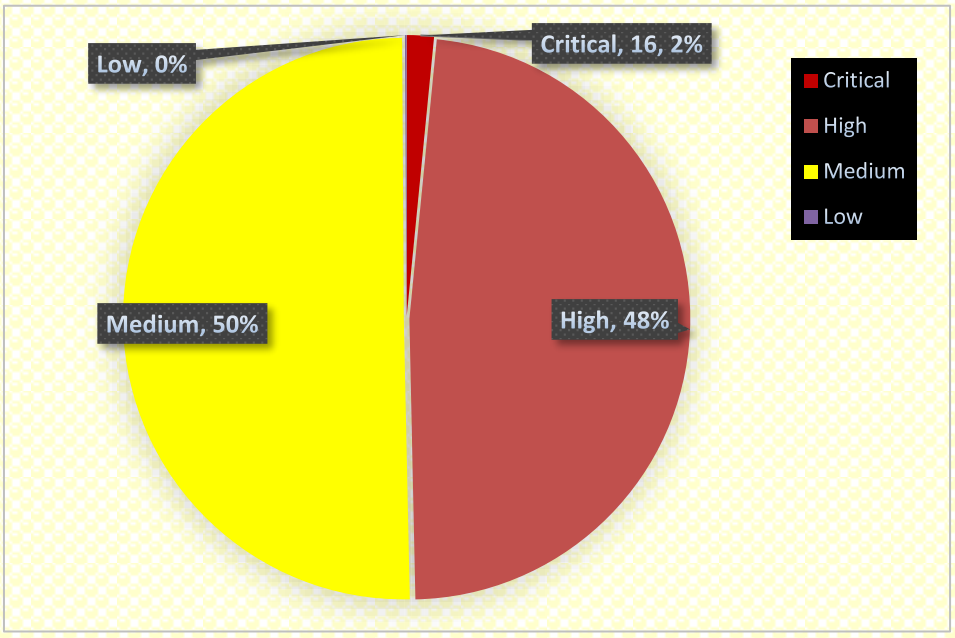
EXECUTIVE SUMMARY

Overall Monthly Vulnerability Trend Chart



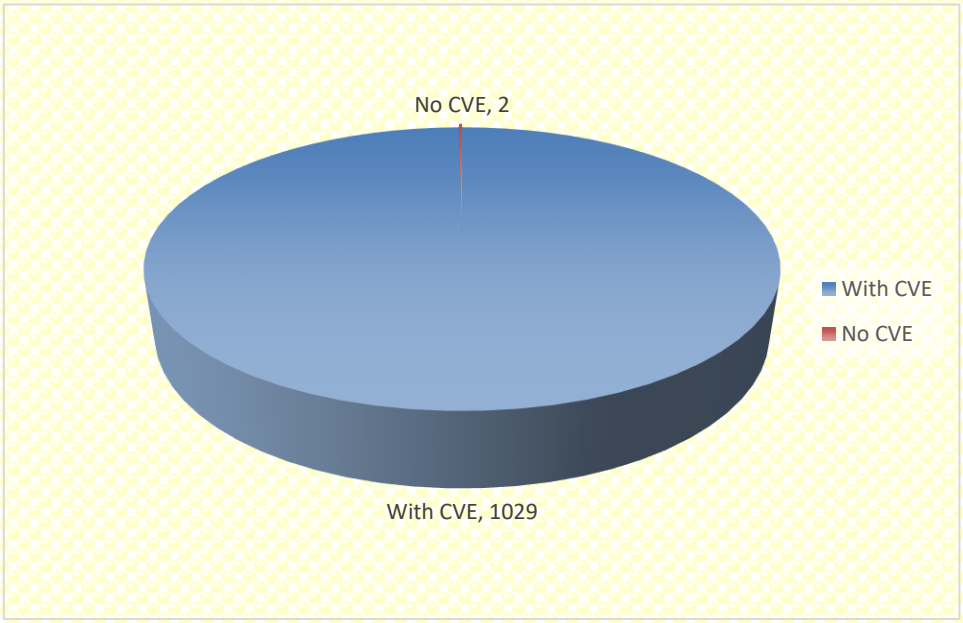
Released Vulnerabilities and Severity Count:

This graph presents threat levels based on vulnerability identified.

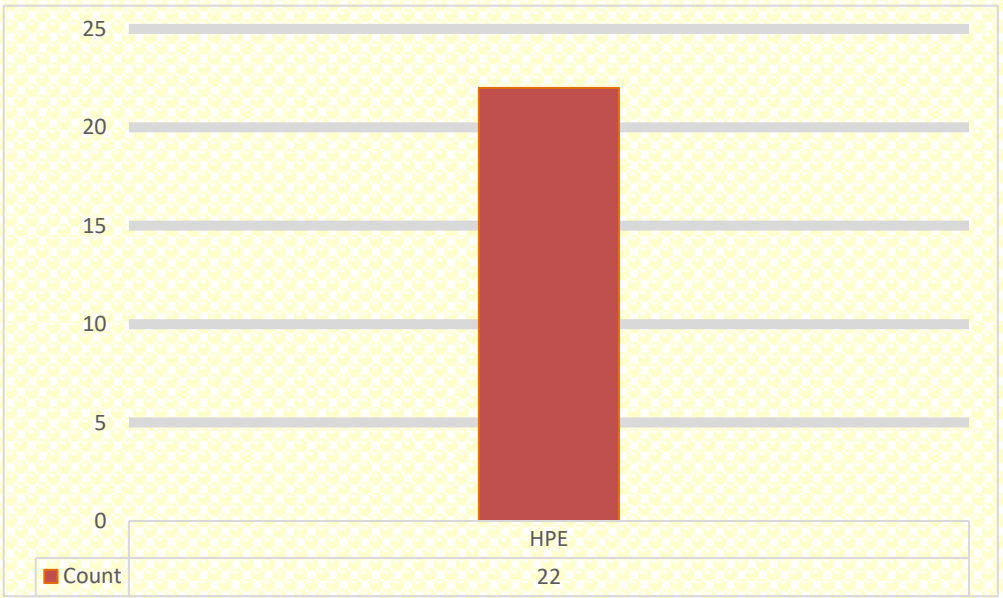


EXECUTIVE SUMMARY

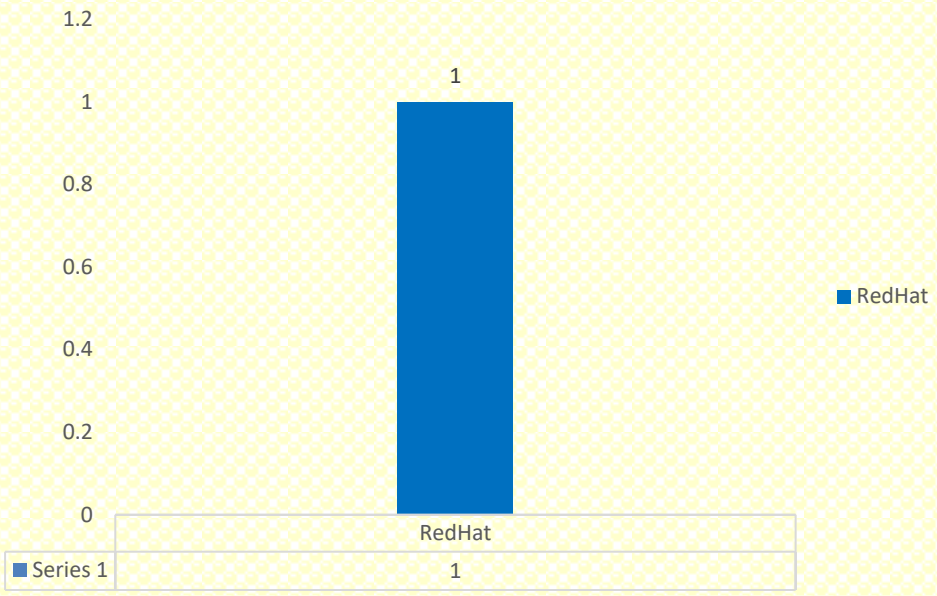
This graph presents the total vulnerabilities released, including zero-day vulnerability with their count.



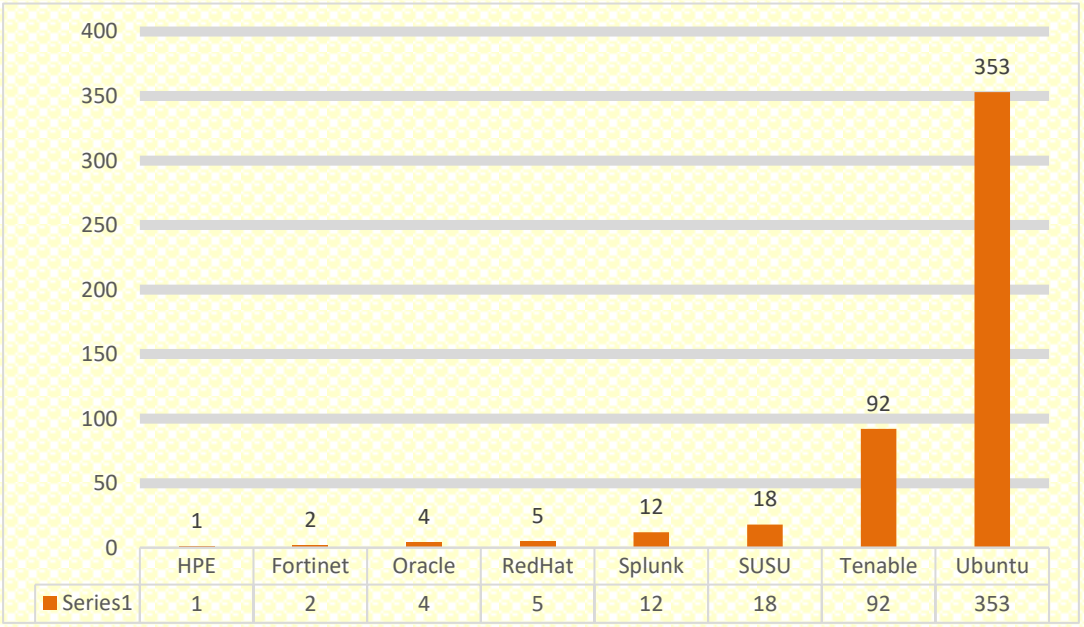
Critical CVE Count: -



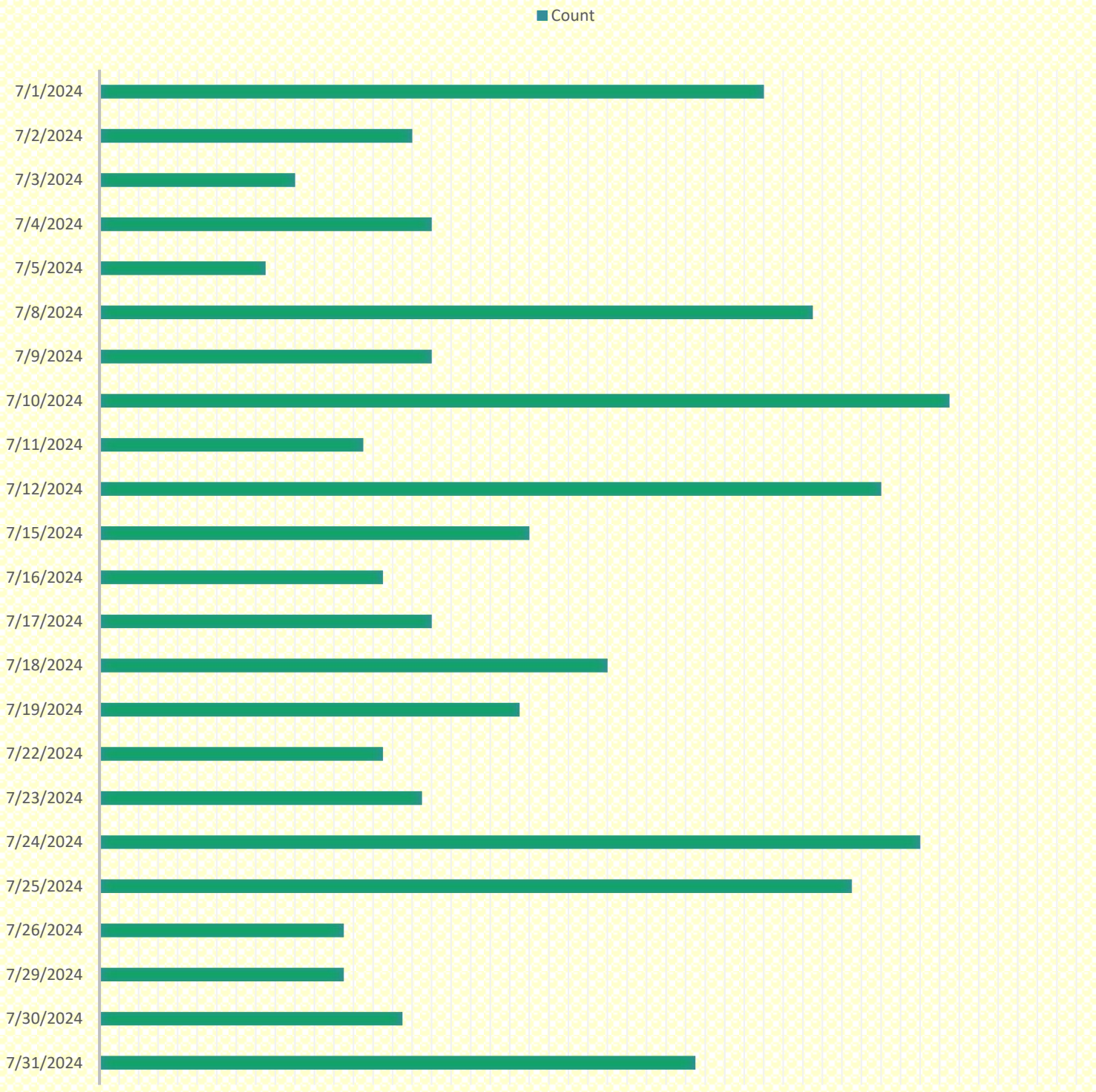
Product-wise Released Non-CVE ID or Zero Day Vulnerabilities Count



HIGH CVE Count: -

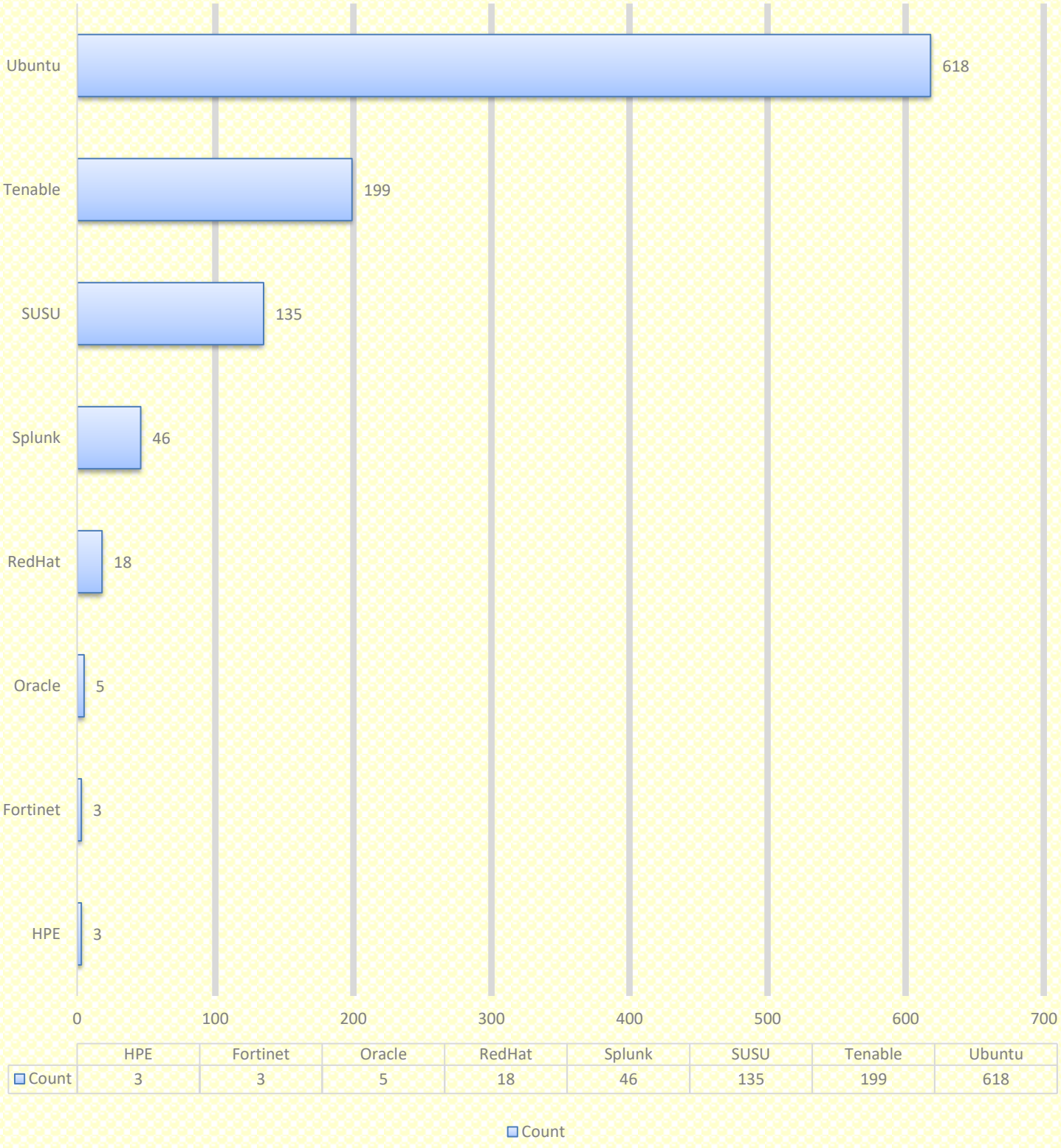


Date-wise Released Vulnerabilities Count, Fortnightly Summarized



	7/31/2024	7/30/2024	7/29/2024	7/26/2024	7/25/2024	7/24/2024	7/23/2024	7/22/2024	7/19/2024	7/18/2024	7/17/2024	7/16/2024	7/15/2024	7/12/2024	7/11/2024	7/10/2024	7/9/2024	7/8/2024	7/5/2024	7/4/2024	7/3/2024	7/2/2024	7/1/2024
Count	61	31	25	25	77	84	33	29	43	52	34	29	44	80	27	87	34	73	17	34	20	32	68

Product-wise Chart for CVE



	HPE	Fortinet	Oracle	RedHat	Splunk	SUSU	Tenable	Ubuntu
Count	3	3	5	18	46	135	199	618

VULNERABILITITIES OF THIS MONTH

Date	SL. No	CVE ID	Vendor	Severity	Summary	Recommendations
1-July	1	CVE-2024-36997	Splunk	Medium	Persistent Cross-site Scripting (XSS) in conf-web/settings REST endpoint	Updates are available please see below reference link: https://advisory.splunk.com/advisories/SVD-2024-0717
	2	CVE-2024-36991	Splunk	High	Path Traversal on the "/modules/messaging/" endpoint in Splunk Enterprise on Windows	Updates are available please see below reference link: https://advisory.splunk.com/advisories/SVD-2024-0711
	3	CVE-2024-36983	Splunk	High	Command Injection using External Lookups	Updates are available please see below reference link: https://advisory.splunk.com/advisories/SVD-2024-0703
	4	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://access.redhat.com/errata/RHSA-2024:1616
	5	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
	6	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
	7	CVE-2022-23820 CVE-2021-46774 CVE-2023-20533 CVE-2023-20519 CVE-2023-20566 CVE-2023-20521 CVE-2021-46766 CVE-2022-23830 CVE-2023-20526 CVE-2021-26345	HPE	Critical	Certain HPE ProLiant DL/XL Servers and HPE Cray Supercomputer Using Certain AMD EPYC Processors, Multiple Vulnerabilities	Updates are available please see below reference link: https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbcr04657en_us&docLocale=en_US
2-July	8	CVE-2023-0464 CVE-2023-0465 CVE-2023-0466 CVE-2023-2650 CVE-2023-3446 CVE-2023-3817 CVE-2023-4807 CVE-2023-5678 CVE-2024-0727 CVE-2023-46218 CVE-2023-46219 CVE-2024-2004 CVE-2024-2398	Tenable	High	Tenable Identity Exposure Version 3.59.5 Fixes Multiple Vulnerabilities	Updates are available please see below reference link: https://www.tenable.com/security/tns-2024-11

		CVE-2024-32974 CVE-2024-32975 CVE-2024-32976 CVE-2024-34362 CVE-2024-34363 CVE-2024-34364 CVE-2024-27983 CVE-2024-22025 CVE-2024-22017 CVE-2024-21892				
	9	CVE-2023-20577	HPE	High	Certain HPE Cray Servers Using Certain AMD EPYC Processors, AMD-SB-7009: AMD Processor Security Notice, Local Arbitrary Code Execution Vulnerability	Updates are available please see below reference link: https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbcr04666en_us&docLocale=en_US
	10	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
	11	CVE-2023-20569	HPE	High	Certain HPE Cray Servers, and HPE ProLiant DL/XL Servers Using Certain AMD EPYC Processors, AMD-SB-7005: Return Address Predictor (INCEPTION) Security Notice, Local Disclosure of Information	Updates are available please see below reference link: https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbcr04545en_us&docLocale=en_US
3-July	12	CVE-2021-47400 CVE-2023-28450 CVE-2023-29483 CVE-2023-34966 CVE-2023-45289 CVE-2023-45290 CVE-2023-52425 CVE-2023-52626 CVE-2023-52667 CVE-2024-2398 CVE-2024-3727 CVE-2024-5037 CVE-2024-24783 CVE-2024-24784 CVE-2024-24785 CVE-2024-24786 CVE-2024-26147 CVE-2024-26801 CVE-2024-26974 CVE-2024-27393 CVE-2024-27397 CVE-2024-27403 CVE-2024-28176 CVE-2024-28757 CVE-2024-35870 CVE-2024-35958 CVE-2024-35960 CVE-2024-36957	RedHat	High	OpenShift Container Platform 4.16.1 bug fix and security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4156
	13	CVE-2024-3657 CVE-2024-2199	Oracle	High	389-ds security update	Updates are available please see below reference link: https://linux.oracle.com/errata/ELSA-2024-4235.html
	14	CVE-2024-24790	Oracle	Medium	go-toolset security update	Updates are available please

		CVE-2024-24789				see below reference link: https://linux.oracle.com/errata/ELSA-2024-4237.html
4-July	15	CVE-2023-7250 CVE-2024-26306	Oracle	Medium	iperf3 security update	Updates are available please see below reference link: https://linux.oracle.com/errata/ELSA-2024-4241.html
	16	CVE-2024-5693 CVE-2024-5691 CVE-2024-5696 CVE-2024-5689 CVE-2024-5690 CVE-2024-5701 CVE-2024-5699 CVE-2024-5697 CVE-2024-5694 CVE-2024-5698 CVE-2024-5695 CVE-2024-5700 CVE-2024-5688	Ubuntu	Medium	Several security issues were fixed in Firefox	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6862-1
	17	CVE-2021-33631 CVE-2024-26898 CVE-2024-24861 CVE-2023-52615 CVE-2024-26720 CVE-2024-2201 CVE-2024-23307 CVE-2023-6270 CVE-2024-26642	Ubuntu	Medium	Linux kernel vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6865-1
	18	CVE-2024-26809 CVE-2024-21823 CVE-2024-26925 CVE-2024-35901 CVE-2024-26924 CVE-2024-26643	Ubuntu	Medium	Linux kernel (Azure) vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6874-1
	19	CVE-2024-26924 CVE-2024-26643 CVE-2024-26925 CVE-2024-26809 CVE-2024-21823	Ubuntu	Medium	Linux kernel (StarFive) vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6873-2
5-July	20	CVE-2023-48945 CVE-2023-31631 CVE-2023-48951 CVE-2023-31630 CVE-2023-31627 CVE-2023-31626 CVE-2023-48947 CVE-2023-31622 CVE-2023-48946 CVE-2023-31629 CVE-2023-48950 CVE-2023-31624 CVE-2023-31620	Ubuntu	Medium	Virtuoso Open-Source Edition vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6879-1
	21	CVE-2024-38439 CVE-2024-38440 CVE-2024-38441	SUSU	High	Security update for netatalk	Updates are available please see below reference link: https://www.suse.com/support/update/announcement/2024/suse-su-20242301-1/
	22	CVE-2024-37370	SUSU	High	Security update for krb5	Updates are available please

		CVE-2024-37371				see below reference link: https://www.suse.com/support/update/announcement/2024/suse-su-20242307-1/
8-July	23	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
	24	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	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

		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				
	25	CVE-2024-38475 CVE-2024-38474 CVE-2024-39573 CVE-2024-38476 CVE-2024-38477 CVE-2024-36387 CVE-2024-39884 CVE-2024-38473	Ubuntu	Medium	Apache HTTP Server vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6885-1
9-July	26	CVE-2024-5458 CVE-2024-5585	Tenable	High	Stand-alone Security Patch Available for Tenable Security Center versions 6.2.1, 6.3.0 and 6.4.0: SC-202407.1	Updates are available please see below reference link: https://www.tenable.com/security/tns-2024-12
	27	CVE-2023-52434 CVE-2024-0193 CVE-2024-26598 CVE-2024-26673 CVE-2024-35890	RedHat	High	kernel security and bug fix update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4415
	28	CVE-2023-52434 CVE-2024-0193 CVE-2024-26673	RedHat	High	kernel-rt security and bug fix update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4412
	29	CVE-2023-45290 CVE-2024-24788 CVE-2024-24784 CVE-2024-24790 CVE-2024-24789 CVE-2023-45289 CVE-2024-24785 CVE-2024-24783 CVE-2023-45288	Ubuntu	Medium	Go vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6886-1
	30	CVE-2024-39330 CVE-2024-39614 CVE-2024-39329 CVE-2024-38875	Ubuntu	High	Django vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6888-1
	31	CVE-2024-26898 CVE-2024-2201 CVE-2024-24861 CVE-2024-23307 CVE-2024-26642 CVE-2024-26736 CVE-2024-26922 CVE-2024-26720 CVE-2021-47063 CVE-2023-52615 CVE-2021-33631 CVE-2023-6270	Ubuntu	Medium	Linux kernel (Azure) vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6866-3
10-July	32	CVE-2021-47293 CVE-2021-47310 CVE-2022-1789	RedHat	High	kernel security update	Updates are available please see below reference link:

		CVE-2024-26583 CVE-2024-26584 CVE-2024-26585 CVE-2024-26735 CVE-2024-26801 CVE-2024-26804 CVE-2024-27397 CVE-2024-35958 CVE-2024-35969 CVE-2024-36005 CVE-2024-36886 CVE-2024-36952				https://access.redhat.com/errata/RHSA-2024:4447
	33	CVE-2024-30105 CVE-2024-35264 CVE-2024-38095	RedHat	High	dotnet8.0 security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4450
	34	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-2022-48624 CVE-2023-2953 CVE-2023-5090 CVE-2023-52464 CVE-2023-52560 CVE-2023-52615 CVE-2023-52626 CVE-2023-52667 CVE-2023-52669 CVE-2023-52675 CVE-2023-52686 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-2024-3651 CVE-2024-4467 CVE-2024-6104 CVE-2024-25629 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	RedHat	Medium	OpenShift Container Platform 4.15.21 bug fix and security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4321

		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-2024-28182 CVE-2024-32487 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				
11-July	35	CVE-2024-30105 CVE-2024-35264 CVE-2024-38095	RedHat	High	dotnet8.0 security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4451
	36	CVE-2023-45229 CVE-2023-45230 CVE-2023-45231 CVE-2023-45232 CVE-2023-45233 CVE-2023-45234 CVE-2023-45235 CVE-2023-45236 CVE-2023-45237	HPE	High	HPE ProLiant DL/DX/ML/SY/RL/XL/Edgeline Servers Using BIOS (PixieFail), Multiple Vulnerabilities	Updates are available please see below reference link: https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04593en_us&docLocale=en_US
	37	CVE-2023-37293 CVE-2023-37297 CVE-2023-37296 CVE-2023-37295 CVE-2023-37294 CVE-2023-3043 CVE-2023-34333 CVE-2023-34332	HPE	Medium	HPE Cray Servers Using AMI MegaRac SPX Software (AMI-SA-2023010), Multiple Vulnerabilities	Updates are available please see below reference link: https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbcr04667en_us&docLocale=en_US
	38	CVE-2022-28656 CVE-2022-28658 CVE-2022-1242 CVE-2022-28654 CVE-2021-3899 CVE-2022-28657 CVE-2022-28655 CVE-2022-28652	Ubuntu	Medium	Apport vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6894-1
12-July	39	CVE-2022-29458 CVE-2022-2509 CVE-2022-29155 CVE-2022-2469 CVE-2022-3821 CVE-2022-4415				

		CVE-2022-45873 CVE-2022-24903 CVE-2022-0934 CVE-2022-27780 CVE-2022-27781 CVE-2022-27782 CVE-2022-22576 CVE-2022-27774 CVE-2022-27775 CVE-2022-27776 CVE-2022-3094 CVE-2022-3736 CVE-2022-3924 CVE-2022-2795 CVE-2022-2881 CVE-2022-2906 CVE-2022-3080 CVE-2022-38177 CVE-2022-38178 CVE-2022-1183 CVE-2022-2928 CVE-2022-2929 CVE-2022-43680 CVE-2022-40674 CVE-2022-27404 CVE-2022-27405 CVE-2022-27406 CVE-2022-31782 CVE-2022-41741 CVE-2022-41742 CVE-2022-3479 CVE-2022-22747 CVE-2022-34480 CVE-2022-40899 CVE-2022-37454 CVE-2022-45061 CVE-2022-42919 CVE-2022-0391 CVE-2022-40090 CVE-2022-48281 CVE-2022-3970 CVE-2022-2519 CVE-2022-2520 CVE-2022-2521 CVE-2022-2867 CVE-2022-2868 CVE-2022-2869 CVE-2022-2953 CVE-2022-34526 CVE-2022-3570 CVE-2022-3597 CVE-2022-3598 CVE-2022-3599 CVE-2022-3627 CVE-2022-1354 CVE-2022-1355 CVE-2022-2056 CVE-2022-2057 CVE-2022-2058 CVE-2020-16156 CVE-2020-19131	HPE	High	HPE Moonshot 1500 Chassis Manager 2.0, Multiple Vulnerabilities	Updates are available please see below reference link: https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04668en_us&docLocale=en_US

		CVE-2020-19144 CVE-2021-39537 CVE-2021-4209 CVE-2021-46823 CVE-2021-46828 CVE-2021-32292 CVE-2021-3618 CVE-2021-4189 CVE-2021-41617 CVE-2021-30560 CVE-2019-17594 CVE-2019-9511 CVE-2019-9513 CVE-2019-17595				
15-July	40	CVE-2021-47548 CVE-2021-47596 CVE-2022-48627 CVE-2023-52638 CVE-2024-26583 CVE-2024-26585 CVE-2024-26720 CVE-2024-26783 CVE-2024-26801 CVE-2024-26852 CVE-2024-35857 CVE-2024-35898 CVE-2024-35969 CVE-2024-36005 CVE-2024-36016 CVE-2024-36886	RedHat	High	kernel security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4533
	41	CVE-2024-29508 CVE-2024-29507 CVE-2024-29511 CVE-2024-29509 CVE-2024-29506	Ubuntu	Medium	Ghostscript vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6897-1
	42	CVE-2024-0727 CVE-2023-5678	HPE	Medium	HPE ProLiant DL/ML/XL, Synergy, Edgeline and Alletra Servers Using OpenSSL, Multiple Vulnerabilities	Updates are available please see below reference link: https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04603en_us&docLocale=en_US
	43	CVE-2023-36617 CVE-2024-27280 CVE-2024-27281 CVE-2024-35176 CVE-2024-27282	Oracle	Medium	ruby security update	Updates are available please see below reference link: https://linux.oracle.com/errata/ELSA-2024-4499.html
	44	CVE-2024-21890 CVE-2023-46809 CVE-2024-22017 CVE-2024-21896 CVE-2024-21892 CVE-2024-21891 CVE-2024-29504 CVE-2024-21509 CVE-2024-21508 CVE-2024-21507 CVE-2024-33883 CVE-2024-21511 CVE-2023-43787 CVE-2023-43786	HPE	Medium	HPE Unified OSS Console Assurance Monitoring (UOCAM), Multiple Vulnerabilities	Updates are available please see below reference link: https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04665en_us&docLocale=en_US

		CVE-2023-43785 CVE-2022-48622 CVE-2023-6597				
16-July	45	CVE-2023-31486 CVE-2023-45229 CVE-2023-45231 CVE-2023-45235 CVE-2023-45236 CVE-2023-45237 CVE-2024-3652 CVE-2024-4418 CVE-2024-6104 CVE-2024-6387 CVE-2024-32002 CVE-2024-32004 CVE-2024-32020 CVE-2024-32021 CVE-2024-32465	RedHat	High	OpenShift Container Platform 4.16.3 security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4469
	46	CVE-2022-27635 CVE-2022-40964 CVE-2022-46329 CVE-2023-20592	RedHat	High	linux-firmware security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4575
	47	CVE-2024-6601 CVE-2024-6603 CVE-2024-6604	Oracle	High	firefox security update	Updates are available please see below reference link: https://linux.oracle.com/errata/ELSA-2024-4517.html
	48	CVE-2024-35264 CVE-2024-38095 CVE-2024-30105	Oracle	High	dotnet8.0 security update	Updates are available please see below reference link: https://linux.oracle.com/errata/ELSA-2024-4450.html
	49	CVE-2024-21131 CVE-2024-21138 CVE-2024-21140 CVE-2024-21145 CVE-2024-21147	RedHat	High	OpenJDK 21.0.4 Security Update for Windows Builds	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4571
17-July	50	CVE-2024-21131 CVE-2024-21138 CVE-2024-21140 CVE-2024-21144 CVE-2024-21145 CVE-2024-21147	RedHat	High	java-11-openjdk security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4564
	51	CVE-2024-21131 CVE-2024-21138 CVE-2024-21140 CVE-2024-21144 CVE-2024-21145 CVE-2024-21147	RedHat	High	OpenJDK 11.0.24 Security Update for Windows Builds	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4565
	52	CVE-2024-6601 CVE-2024-6603 CVE-2024-6604	RedHat	High	firefox security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4586

	53	CVE-2024-6601 CVE-2024-6603 CVE-2024-6604	RedHat	High	firefox security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4590
	54	CVE-2023-3128 CVE-2023-4822 CVE-2023-6597 CVE-2023-43646 CVE-2023-47108 CVE-2023-49568 CVE-2023-49569 CVE-2024-0450 CVE-2024-1394 CVE-2024-5042 CVE-2024-24783 CVE-2024-24785 CVE-2024-24786 CVE-2024-28176 CVE-2024-28180 CVE-2024-28863 CVE-2024-37890	RedHat	High	Red Hat OpenShift Data Foundation 4.16.0 security, enhancement & bug fix update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4591
18-July	55	CVE-2024-21131 CVE-2024-21140 CVE-2024-21145 CVE-2024-21147 CVE-2024-21138	Oracle	High	java-17-openjdk security update	Updates are available please see below reference link: https://linux.oracle.com/errata/ELSA-2024-4568.html
	56	CVE-2024-6601 CVE-2024-6603 CVE-2024-6604	RedHat	High	thunderbird security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4635
	57	CVE-2024-6601 CVE-2024-6603 CVE-2024-6604	RedHat	High	firefox security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4634
	58	CVE-2024-1062 CVE-2024-2199 CVE-2024-3657 CVE-2024-5953	RedHat	High	389-ds-base security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4633
	59	CVE-2022-48624 CVE-2023-2953 CVE-2023-45288 CVE-2023-45289 CVE-2023-45290 CVE-2024-24783 CVE-2024-24786 CVE-2024-25062 CVE-2024-25620 CVE-2024-26147 CVE-2024-28182 CVE-2024-32002 CVE-2024-32004 CVE-2024-32020 CVE-2024-32021 CVE-2024-32465 CVE-2024-32487	RedHat	Medium	Errata Advisory for Red Hat OpenShift GitOps v1.11.6 security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4626

		CVE-2024-33599 CVE-2024-33600 CVE-2024-33601 CVE-2024-33602				
19-July	60	CVE-2024-2398 CVE-2024-2961 CVE-2024-3651 CVE-2024-6387 CVE-2024-21011 CVE-2024-21012 CVE-2024-21068 CVE-2024-21085 CVE-2024-21094 CVE-2024-24806 CVE-2024-25062 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-2024-28182 CVE-2024-28757 CVE-2024-28834 CVE-2024-28835 CVE-2024-30105 CVE-2024-32002 CVE-2024-32004 CVE-2024-32020 CVE-2024-32021 CVE-2024-32465 CVE-2024-32487 CVE-2024-33599 CVE-2024-33600 CVE-2024-33601 CVE-2024-33602 CVE-2024-35235 CVE-2024-35264 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	RedHat	High	Red Hat OpenShift Dev Spaces 3.15.0 release	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4631

		CVE-2024-35960 CVE-2024-36004 CVE-2024-36007 CVE-2024-38095				
22-July	61	CVE-2024-23663	Fortinet	High	Privilege escalation from low privilege administrator	Updates are available please see below reference link: https://www.fortiguard.com/psirt/FG-IR-23-459
	62	CVE-2024-26015	Fortinet	Low	IP address validation mishandles zero characters	Updates are available please see below reference link: https://www.fortiguard.com/psirt/FG-IR-23-446
	63	CVE-2024-26006	Fortinet	Medium	Cross site scripting vulnerability in SSL VPN web UI	Updates are available please see below reference link: https://www.fortiguard.com/psirt/FG-IR-23-485
	64	CVE-2024-6602 CVE-2024-6601 CVE-2024-6600 CVE-2024-6604 CVE-2024-6603	Ubuntu	Medium	Thunderbird vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6903-1
	65	CVE-2024-1975 CVE-2024-1737 CVE-2024-0760 CVE-2024-4076	Ubunru	Medium	Bind vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6909-1
	66	CVE-2021-26117 CVE-2022-41678 CVE-2023-46604 CVE-2020-13920 CVE-2018-11775 CVE-2015-7559	Ubuntu	Medium	Apache ActiveMQ vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6910-1
	67	CVE-2024-6601 CVE-2024-6602 CVE-2024-6603 CVE-2024-6604	RedHat	High	thunderbird security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4670
	68	CVE-2024-6601 CVE-2024-6603 CVE-2024-6604	RedHat	High	firefox security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4673
	69	CVE-2024-38473 CVE-2024-38474 CVE-2024-38475 CVE-2024-38477 CVE-2024-39573	RedHat	High	httpd:2.4 security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4720
23-July	70	CVE-2024-33519 CVE-2024-41133 CVE-2024-41134 CVE-2024-41135 CVE-2024-41136 CVE-2023-51385 CVE-2023-48795	HPE	High	HPE Aruba Networking EdgeConnect SD-WAN, Multiple Vulnerabilities	Updates are available please see below reference link: https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04673en_us&docLocale=en_US
	71				HPE Aruba Networking	Updates are available please see below reference

		CVE-2024-22443 CVE-2024-22444 CVE-2024-41914	HPE	Critical	EdgeConnect SD-WAN Orchestrator, Multiple Vulnerabilities	link: https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04672en_us&docLocale=en_US
	72	CVE-2024-29131 CVE-2024-29133 CVE-2017-16137 CVE-2024-21512 CVE-2023-48161 CVE-2023-39742 CVE-2023-48622 CVE-2024-21490 CVE-2022-37052 CVE-2022-37051 CVE-2022-37050 CVE-2021-37623 CVE-2021-37622 CVE-2021-37621 CVE-2021-37620 CVE-2021-37616 CVE-2021-37615 CVE-2021-34335 CVE-2021-34334 CVE-2021-32815 CVE-2020-23922	HPE	High	HPE Unified OSS Console Assurance Monitoring (UOCAM), Multiple Vulnerabilities	Updates are available please see below reference link: https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04670en_us&docLocale=en_US
	73	CVE-2021-25329 CVE-2020-9484 CVE-2019-0221	Ubuntu	Medium	Tomcat vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6908-1
24-July	74	CVE-2022-36765 CVE-2023-45236 CVE-2023-45237	Oracle	Medium	edk2 security update	Updates are available please see below reference link: https://linux.oracle.com/errata/ELSA-2024-4749.html
	75	CVE-2024-38474 CVE-2024-38475 CVE-2024-38477	RedHat	High	httpd:2.4 security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4830
	76	CVE-2024-38474 CVE-2024-38475 CVE-2024-38477	RedHat	High	httpd:2.4 security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4827
	77	CVE-2024-38474 CVE-2024-38475 CVE-2024-38477	RedHat	High	httpd:2.4 security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4820
	78	CVE-2020-26555 CVE-2021-46909 CVE-2021-46972 CVE-2021-47069 CVE-2021-47073 CVE-2021-47236 CVE-2021-47310 CVE-2021-47311	RedHat	Medium	security update Logging for Red Hat OpenShift - 5.6.21	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4336

		CVE-2021-47353 CVE-2021-47356 CVE-2021-47456 CVE-2021-47495 CVE-2022-48624 CVE-2023-2953 CVE-2023-5090 CVE-2023-52464 CVE-2023-52560 CVE-2023-52615 CVE-2023-52626 CVE-2023-52667 CVE-2023-52669 CVE-2023-52675 CVE-2023-52686 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-2024-24790 CVE-2024-24806 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-2024-28182 CVE-2024-32002 CVE-2024-32004 CVE-2024-32020 CVE-2024-32021 CVE-2024-32465 CVE-2024-32487 CVE-2024-35235 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	RedHat	Medium	security update Logging for Red Hat OpenShift - 5.6.21	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4336

		CVE-2024-35959 CVE-2024-35960 CVE-2024-36004 CVE-2024-36007				
25-July	79	CVE-2023-6597 CVE-2024-0450 CVE-2024-6535	RedHat	Medium	Red Hat Service Interconnect security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4865
	80	CVE-2024-38474 CVE-2024-38475 CVE-2024-38477	RedHat	High	httpd security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4863
	81	CVE-2021-47548 CVE-2021-47596 CVE-2022-41723 CVE-2022-48627 CVE-2022-48743 CVE-2023-6597 CVE-2023-22745 CVE-2023-27522 CVE-2023-28450 CVE-2023-31346 CVE-2023-31486 CVE-2023-45229 CVE-2023-45231 CVE-2023-45235 CVE-2023-45236 CVE-2023-45237 CVE-2023-45288 CVE-2023-52638 CVE-2023-52667 CVE-2023-52784 CVE-2024-0450 CVE-2024-2398 CVE-2024-3651 CVE-2024-3652 CVE-2024-4418 CVE-2024-4467 CVE-2024-5564 CVE-2024-6387 CVE-2024-26583 CVE-2024-26585 CVE-2024-26720 CVE-2024-26733 CVE-2024-26783 CVE-2024-26801 CVE-2024-26852 CVE-2024-26908 CVE-2024-28182 CVE-2024-32002 CVE-2024-32004 CVE-2024-32020 CVE-2024-32021 CVE-2024-32465 CVE-2024-32487 CVE-2024-35857 CVE-2024-35898 CVE-2024-35960 CVE-2024-35969	Redaht	High	OpenShift Container Platform 4.12.61 bug fix and security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4677

		CVE-2024-36005 CVE-2024-36016 CVE-2024-36020 CVE-2024-36025 CVE-2024-36886 CVE-2024-36924 CVE-2024-36929 CVE-2024-38596 CVE-2024-39936				
	82	CVE-2024-23638 CVE-2024-37894	Oracle	Medium	squid security update	Updates are available please see below reference link: https://linux.oracle.com/errata/ELSA-2024-4861.html
26-July	83	CVE-2020-28241 CVE-2021-46848 CVE-2022-36227 CVE-2022-47629 CVE-2022-48624 CVE-2023-2953 CVE-2023-3446 CVE-2023-3817 CVE-2023-4016 CVE-2023-4408 CVE-2023-5678 CVE-2023-6004 CVE-2023-6597 CVE-2023-6918 CVE-2023-7104 CVE-2023-32681 CVE-2023-50387 CVE-2023-50868 CVE-2024-0450 CVE-2024-3651 CVE-2024-24806 CVE-2024-25062 CVE-2024-28182 CVE-2024-28834 CVE-2024-32002 CVE-2024-32004 CVE-2024-32020 CVE-2024-32021 CVE-2024-32465 CVE-2024-32487 CVE-2024-33599 CVE-2024-33600 CVE-2024-33601 CVE-2024-33602 CVE-2024-40634	RedHat	High	Errata Advisory for Red Hat OpenShift GitOps v1.13.1 security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4891
	84	CVE-2018-3613 CVE-2018-12183 CVE-2019-0160 CVE-2017-5731 CVE-2018-12182	Ubuntu	Medium	EDK II vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6920-1
29-July	85	CVE-2024-24858 CVE-2024-25739 CVE-2024-24857 CVE-2024-24859	Ubuntu	Medium	Linux kernel vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6922-1

	86	CVE-2023-45290 CVE-2024-24783 CVE-2024-24785 CVE-2024-24790	RedHat	Medium	rhc-worker-script security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4893
	87	CVE-2024-6601 CVE-2024-6602 CVE-2024-6603 CVE-2024-6604	RedHat	High	thunderbird security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4894
	88	CVE-2021-47548 CVE-2022-48743 CVE-2023-52667 CVE-2023-52784 CVE-2024-26733 CVE-2024-26852 CVE-2024-26908 CVE-2024-35960 CVE-2024-36020 CVE-2024-36025 CVE-2024-36924 CVE-2024-36929 CVE-2024-38596	RedHat	Medium	kernel security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4902
30-July	89	CVE-2024-38474 CVE-2024-38475 CVE-2024-38477	RedHat	High	httpd security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4938
	90	CVE-2024-4741 CVE-2024-2511 CVE-2024-5535 CVE-2024-4603	Ubuntu	Medium	OpenSSL vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6937-1
	91	CVE-2024-21165 CVE-2024-21171 CVE-2024-20996 CVE-2024-21173 CVE-2024-21179 CVE-2024-21130 CVE-2024-21185 CVE-2024-21162 CVE-2024-21142 CVE-2024-21125 CVE-2024-21163 CVE-2024-21127 CVE-2024-21177 CVE-2024-21129 CVE-2024-21134	Ubuntu	Medium	MySQL vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6934-1
	92	CVE-2024-21147 CVE-2024-21140 CVE-2024-21145 CVE-2024-21138 CVE-2024-21131	Ubuntu	Medium	OpenJDK 21 vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6932-1
	93	CVE-2024-27017 CVE-2024-26952 CVE-2024-25742 CVE-2024-26886 CVE-2023-52752 CVE-2024-36016	Ubuntu	Medium	Linux kernel vulnerabilities	Updates are available please see below reference link: https://ubuntu.com/security/notices/USN-6923-2
31-July		CVE-2021-47459				

		CVE-2022-36402 CVE-2022-38457 CVE-2022-40133 CVE-2022-48743 CVE-2023-5633 CVE-2023-27522 CVE-2023-29483 CVE-2023-33951 CVE-2023-33952 CVE-2023-45289 CVE-2023-45290 CVE-2023-52434 CVE-2023-52439 CVE-2023-52450 CVE-2023-52518 CVE-2023-52578 CVE-2023-52707 CVE-2023-52811 CVE-2024-1151 CVE-2024-3727 CVE-2024-5564 CVE-2024-6104 CVE-2024-6409 CVE-2024-24783 CVE-2024-24784 CVE-2024-24785 CVE-2024-24786 CVE-2024-26581 CVE-2024-26668 CVE-2024-26698 CVE-2024-26704 CVE-2024-26739 CVE-2024-26773 CVE-2024-26808 CVE-2024-26810 CVE-2024-26880 CVE-2024-26908 CVE-2024-26923 CVE-2024-26925 CVE-2024-26929 CVE-2024-26931 CVE-2024-26982 CVE-2024-27016 CVE-2024-27019 CVE-2024-27020 CVE-2024-27065 CVE-2024-27417 CVE-2024-28176 CVE-2024-32487 CVE-2024-35791 CVE-2024-35897 CVE-2024-35899 CVE-2024-35950 CVE-2024-36025 CVE-2024-36489 CVE-2024-36904 CVE-2024-36924 CVE-2024-36952 CVE-2024-36978 CVE-2024-38596 CVE-2024-39936	RedHat	Medium	OpenShift Container Platform 4.13.46 security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:4846

SOME ZERO-DAY VULNERABILITITIES OF THE MONTH

SL. N0	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
02				

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**