

SECURITY INTELLIGENCE ADVISORY

01st Feb 2024 – 29th Feb 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.

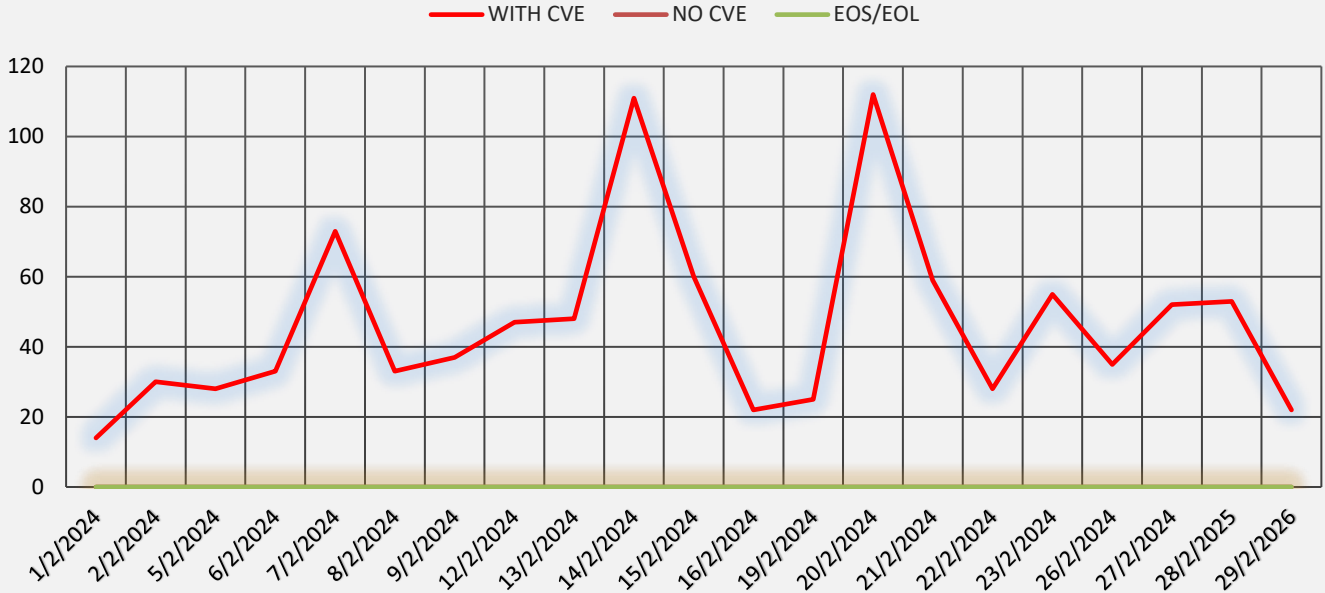
One effective way to stay on top of these vulnerabilities is by conducting regular vulnerability assessments. These periodic assessments cover your entire IT infrastructure and help you identify new threats that may have emerged. This proactive practice enables you to stay abreast of the current state 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 Satrix Research Team are those in use in the customers' environment.
 - If customers use products that aren't already being monitored by our team, they can be submitted to us, and we will initiate monitoring them the next business day. We only monitor public or commercially available solutions.
 - The Vulnerability Database covers vulnerabilities that can be exploited in all types of products – software, hardware, firmware, etc.
 - The vulnerabilities verified by our team are described in the client database as an Advisory and listed in the Satrix Vulnerability Reports, detailing what IT Security teams need to know to mitigate the risk posed by the vulnerability in their environment.
 - The Vulnerability Database covers vulnerabilities that can be exploited in all types of products. We also cover zero days and eos/eol.
 - We create daily and weekly reports covering all the details about detected vulnerabilities and the total vulnerability count in the last week and provide them to customers.
 - The Satrix Advisory descriptions include severity, under investigation product, Affected Product, CVE ID, Satrix score, reference links, and remediation recommendations.
 - Satrix researchers complete the vulnerability assessment process within 5 business working days.
-

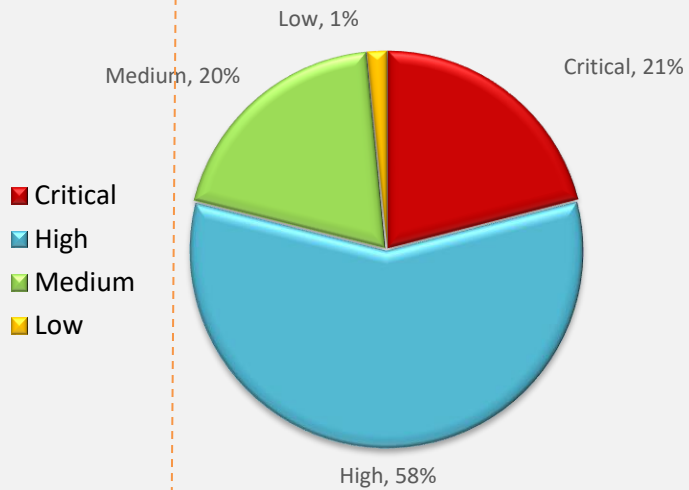
EXECUTIVE SUMMARY

Overall Monthly Vulnerability Trend Chart



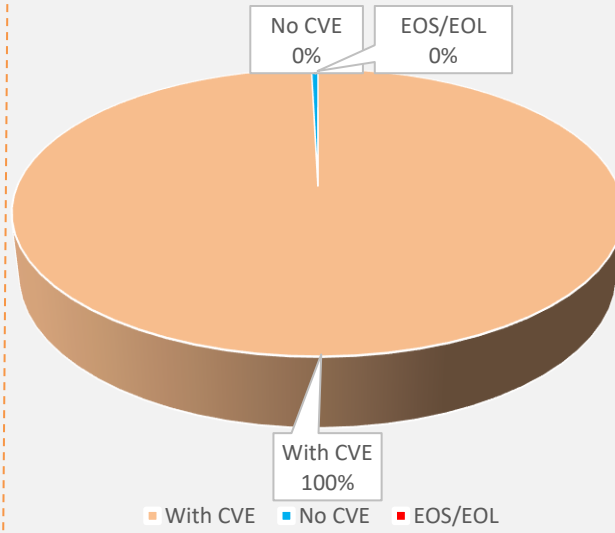
Released Vulnerabilities and Severity Count:

This graph presents threat levels based on vulnerability identified.

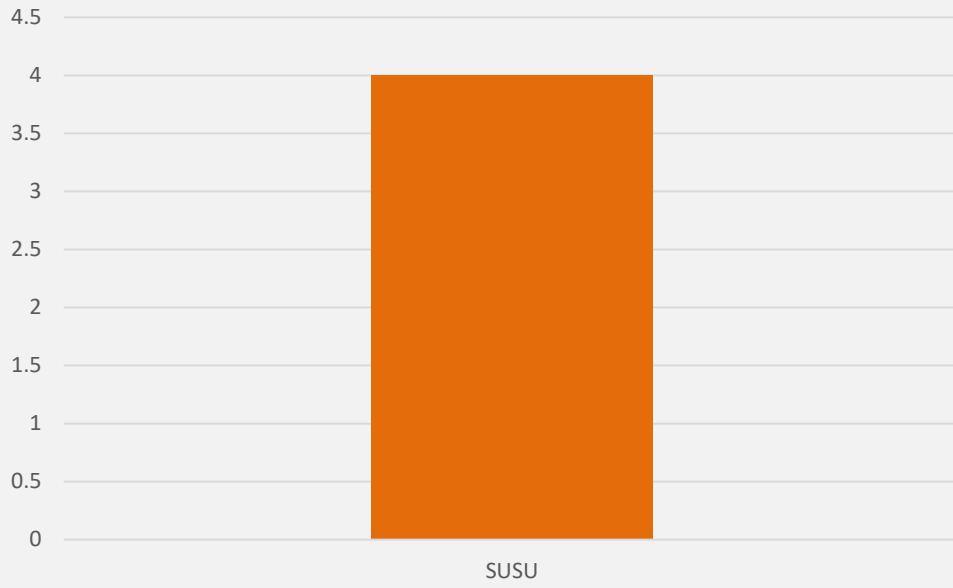


EXECUTIVE SUMMARY

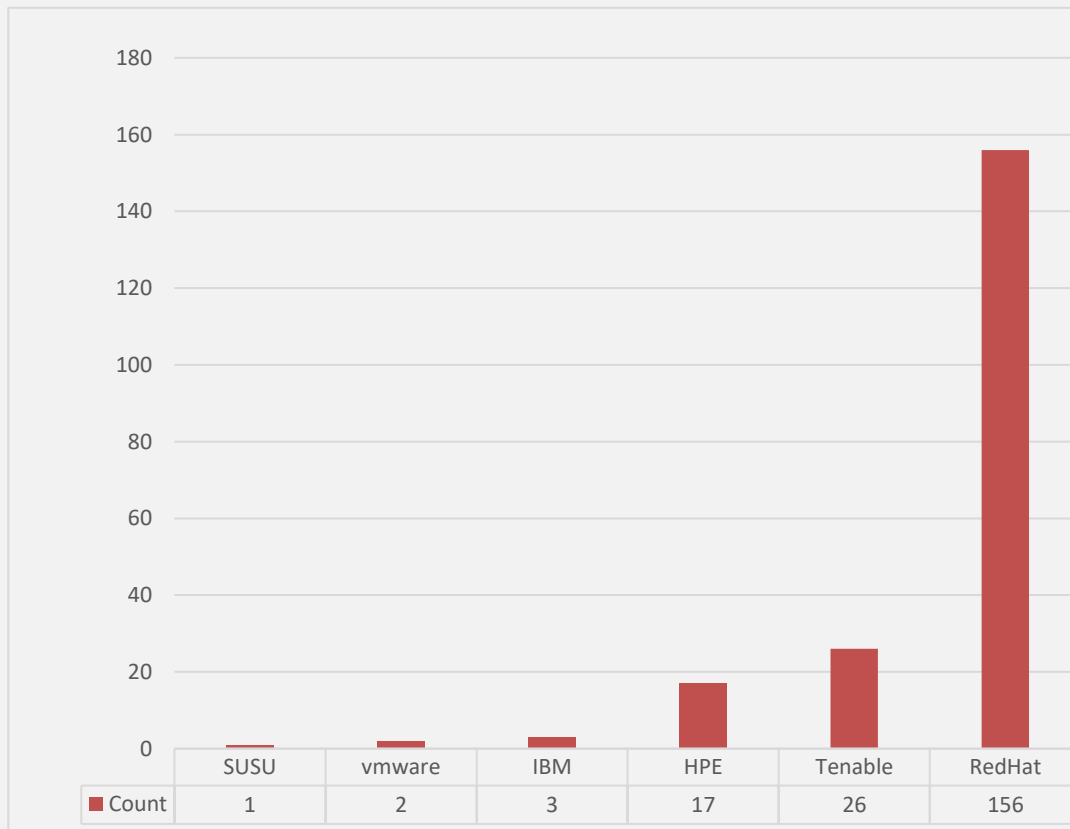
This graph presents the total vulnerabilities released, including zero-day vulnerability and EOS/EOL, with their count.



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

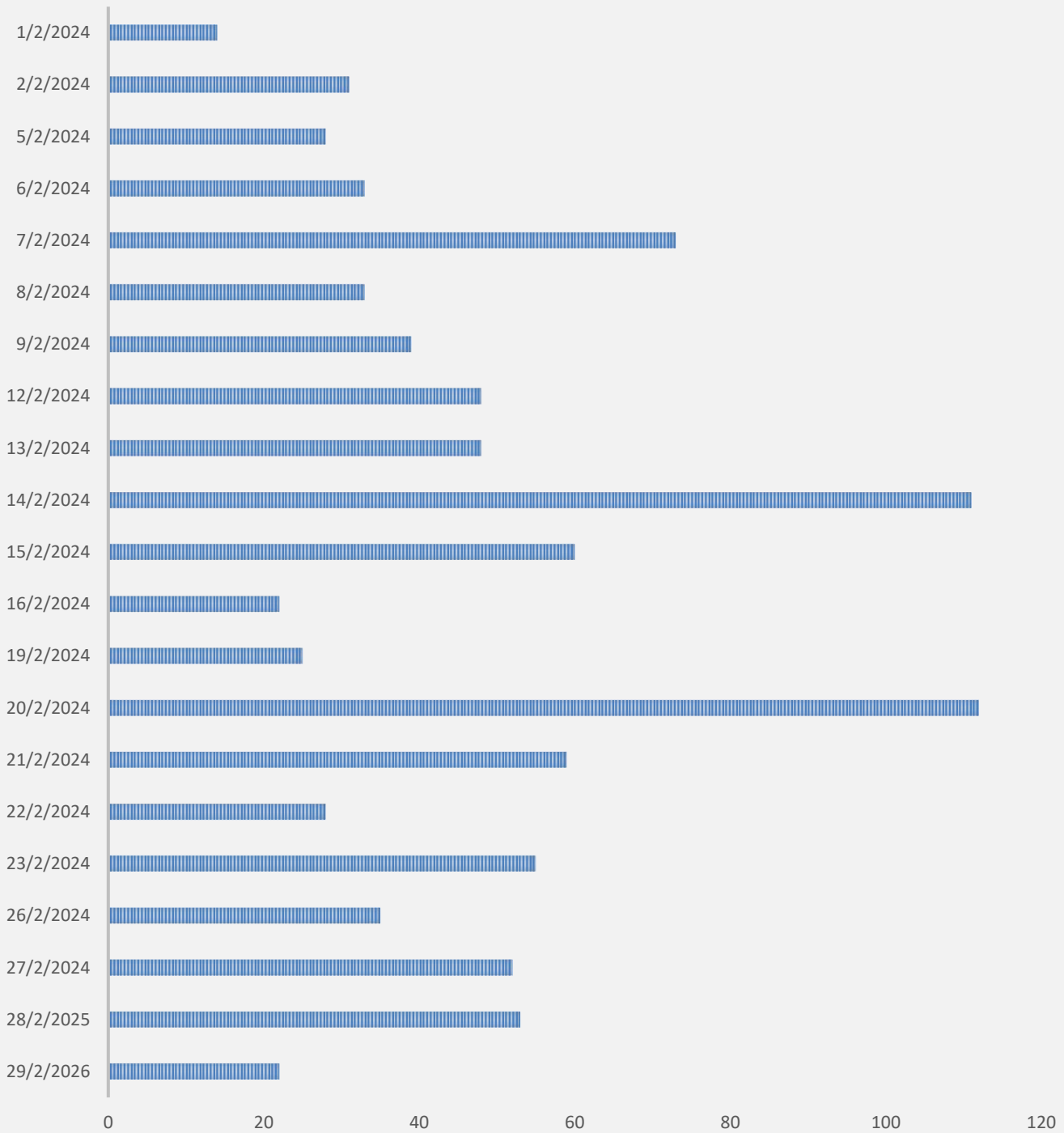


Critical CVE Count



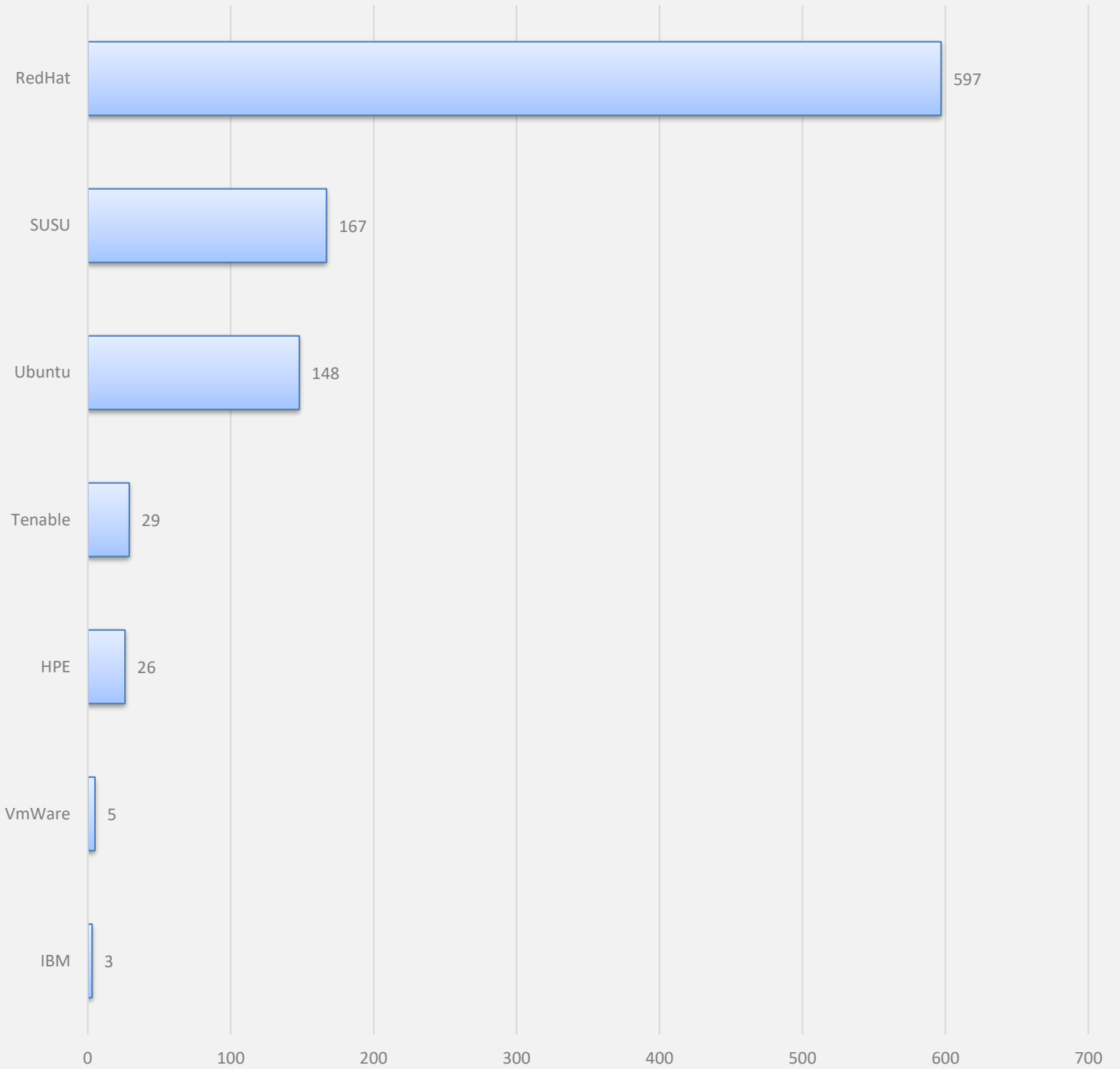
Date-wise Released Vulnerabilities Count, Fortnightly Summarized

■ Count



■ Count	22	53	52	35	55	28	59	112	25	22	60	111	48	48	39	33	73	33	28	31	14
---------	----	----	----	----	----	----	----	-----	----	----	----	-----	----	----	----	----	----	----	----	----	----

Product-wise Chart for CVE



	IBM	VmWare	HPE	Tenable	Ubuntu	SUSU	RedHat
Count	3	5	26	29	148	167	597

Count

TOP VULNERABILITIES OF THE MONTH

DATE	CVE ID	Vendor	Summary	Recommendation
05-02-24	CVE-2023-39325 CVE-2023-45142 CVE-2023-47108 CVE-2023-49568 CVE-2023-49569	RedHat	OpenShift Container Platform 4.14.11 bug fix and security update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:0642
06-02-24	CVE-2023-2976 CVE-2020-8908 CVE-2023-46589 CVE-2023-20863 CVE-2016-3088 CVE-2023-46604 CVE-2020-27853 CVE-2021-41093 CVE-2017-7657 CVE-2017-7658 CVE-2023-44981 CVE-2023-20862 CVE-2023-20861 CVE-2022-42004 CVE-2022-42003 CVE-2022-25883 CVE-2023-28155	HPE	HPE Unified OSS Console Assurance Monitoring (UOCAM), Multiple Vulnerabilities	Updates are available please see below reference link: https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04590en_us
08-02-24	CVE-2023-49568 CVE-2023-49569	RedHat	Red Hat Advanced Cluster Management 2.7.11 security and bug fix container update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2024:0729
15-02-24	CVE-2023-36665	IBM	QRadar Suite Software includes components with multiple known vulnerabilities	Updates are available please see below reference link: https://www.ibm.com/support/pages/node/7118351
22-02-24	CVE-2024-22245 CVE-2024-22250	VMWare	Addressing Arbitrary Authentication Relay and Session Hijack Vulnerabilities in Deprecated VMware Enhanced Authentication Plug-in	Updates are available please see below reference link: https://www.vmware.com/security/advisories/VMSA-2024-0003.html
23-02-24	CVE-2024-0057 CVE-2024-20672	Tenable	Tenable Identity Exposure Version 3.59.4 Fixes Multiple Vulnerabilities	Updates are available please see below reference link: https://www.tenable.com/security/tns-2024-04
28-02-24	CVE-2021-35937 CVE-2021-35938 CVE-2021-35939 CVE-2023-3978 CVE-2023-5363 CVE-2023-5981 CVE-2023-27043 CVE-2023-39325 CVE-2023-39326 CVE-2023-45142	Redhat	OpenShift Container Platform 4.15.0 security and extras update	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2023:7197

Disclaimer: The information in this document is subject to change without notice and should not be construed as a commitment by Satrix Information Security (P) Ltd. Satrix provides no warranty, express or implied, including warranties of merchantability and information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall Satrix or any of its suppliers be liable for direct, indirect, special, incidental, or consequential damages of any nature or kind arising from the use of this document or the use of any hardware or software described in this document, even if Satrix or its suppliers have been advised of the possibility of such damages. This document and parts hereof must not be reproduced or copied without written permission from Satrix, and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose. All rights to registrations and trademarks reside with their respective owners © Copyright 2013-2022 Satrix. All rights reserved.

Limitation of Liability: IN NO EVENT SHALL Satrix, Satrix AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD-PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF Satrix HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Global Presence

USA / Satrix Information Security Incorporation

UK/EU / Satrix Info Security Ltd

MEA / Satrix Information Security DMCC

India / Satrix Information Security 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@satrix.com

www.satrix.com

