Gattrix

SECURITY INTELLIGENCE ADVISORY

25th Aug 2022 - 24th Sep 2022

INTENT

This report is intended to help quantify the scope of that risk as organizations' struggle to balance their cyber security policies and protections against the needs of their employees for access to the Web and its resources.

BACKGROUND

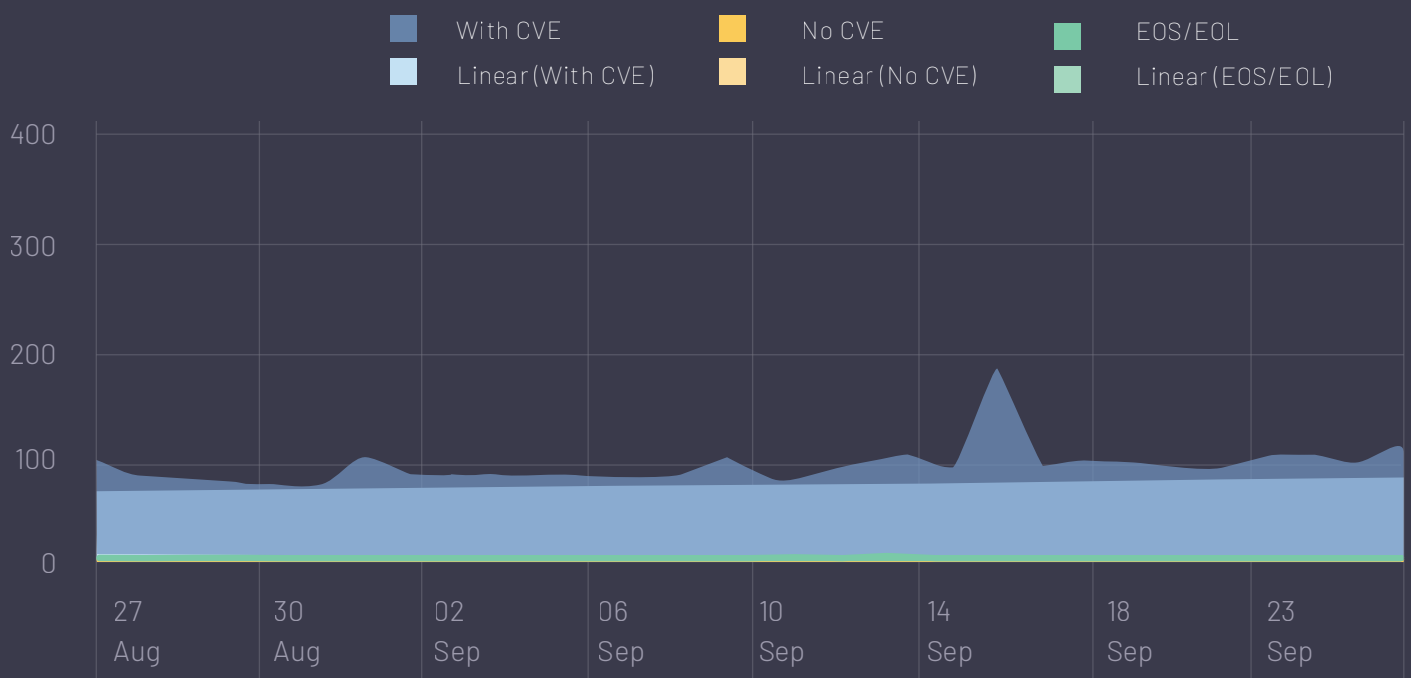
Every organization – large, medium and small has a huge risk and a typical challenge of managing vulnerabilities present in the operating systems, Vulnerabilities that are not attended possess a very high risk and can cost your organization various threats and damage. There is threat from users within the system, competitors who want to know accurate details about your business model etc. There is a certain way to identify and update patches for your vulnerabilities to avoid all these serious threats and curb the damage thereof. There's also a method in which specialists get into your system and run a check to identify how strong the system is. Performing vulnerability assessments guarantee all normal system vulnerabilities are taken into consideration. When assessments are conducted regularly, new threats are identified quickly.

WHAT DOES THE VULNERABILITY ADVISORY COVER?

- We monitor around 2000 applications, appliances and operating systems, and tests and verifies the vulnerabilities reported in them.
- We are focusing each vulnerability disclosed in those 2000 products.
- The systems and applications monitored by Sattrix Research Team are those in use in the environment of the customers.
- In the instance of customers using products that aren't already being monitored by our team, these products 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 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 and also, we cover zero days and eos/eol.
- We create daily and weekly reports including all the details of that vulnerability and total vulnerability count in last week and provide it to customer as well.
- The Sattrix Advisory descriptions include severity, under investigation product, Affected Product, cve id, Sattrix score, reference links and remediations.
- Sattrix researchers monitor the vulnerabilities within 5 business working days.

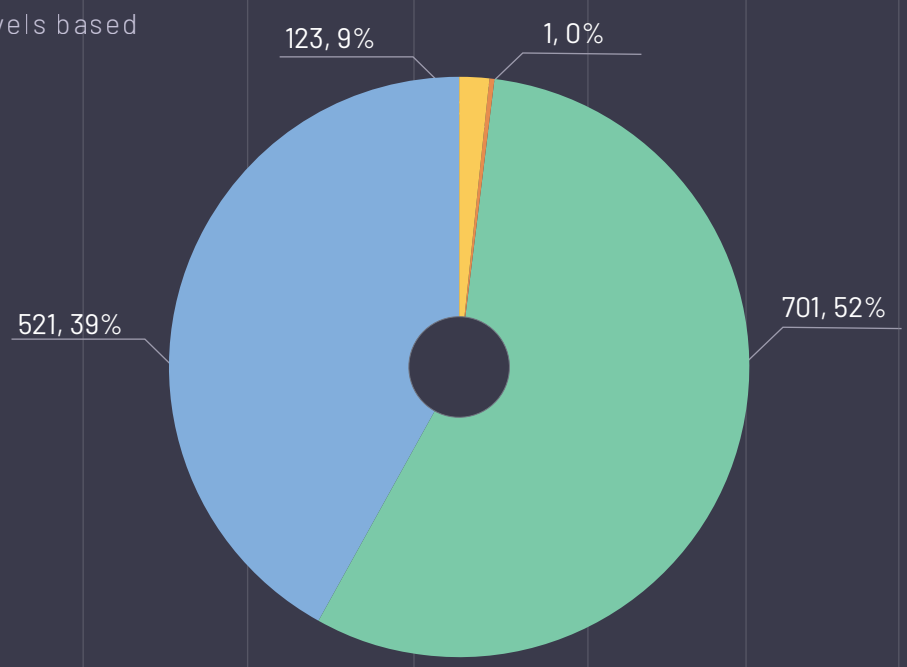
EXECUTIVE SUMMARY

Overall Monthly Vulnerability Trend Chart



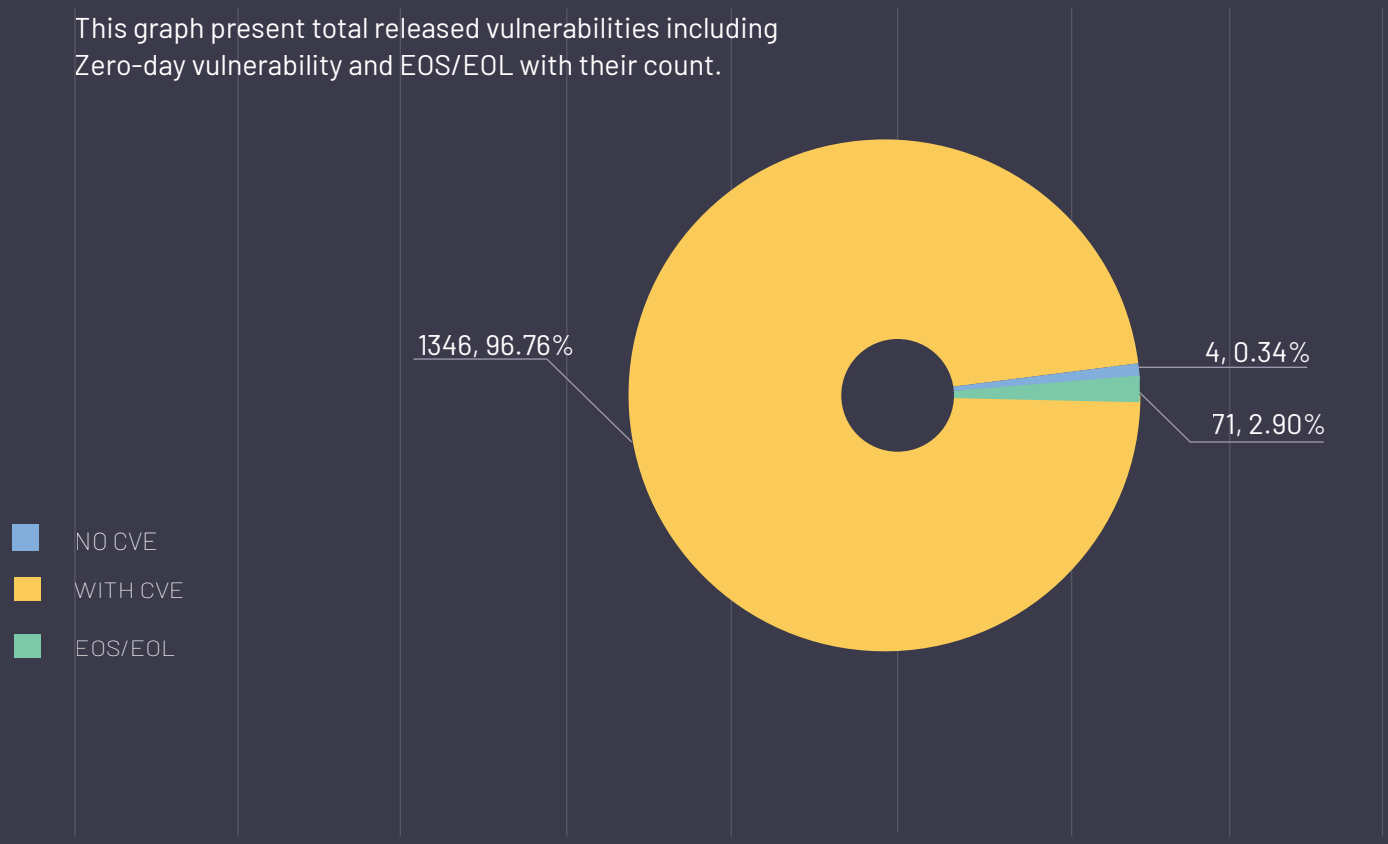
Released Vulnerabilities and severity wise count low severity count

This graph present threat levels based on vulnerability identified.

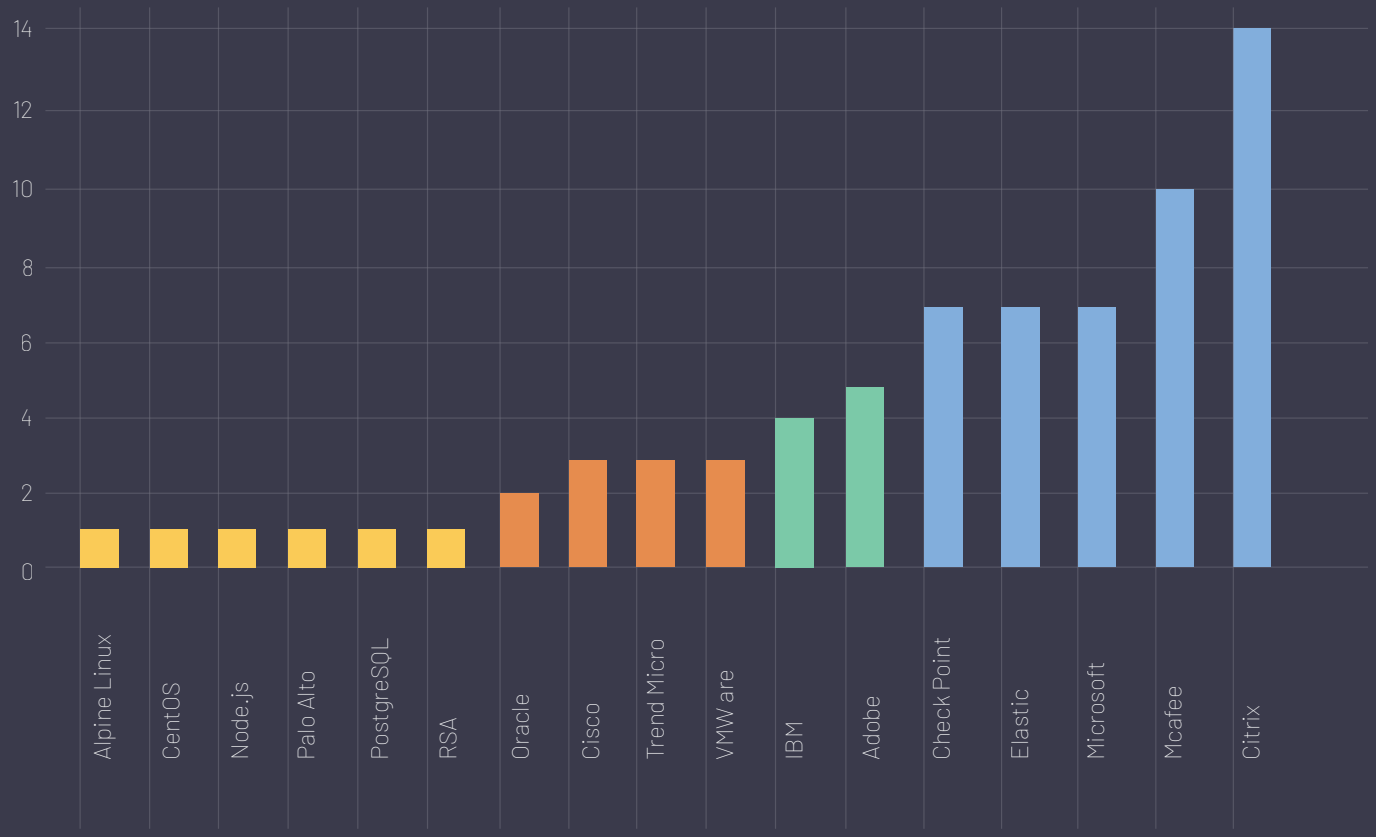


EXECUTIVE SUMMARY

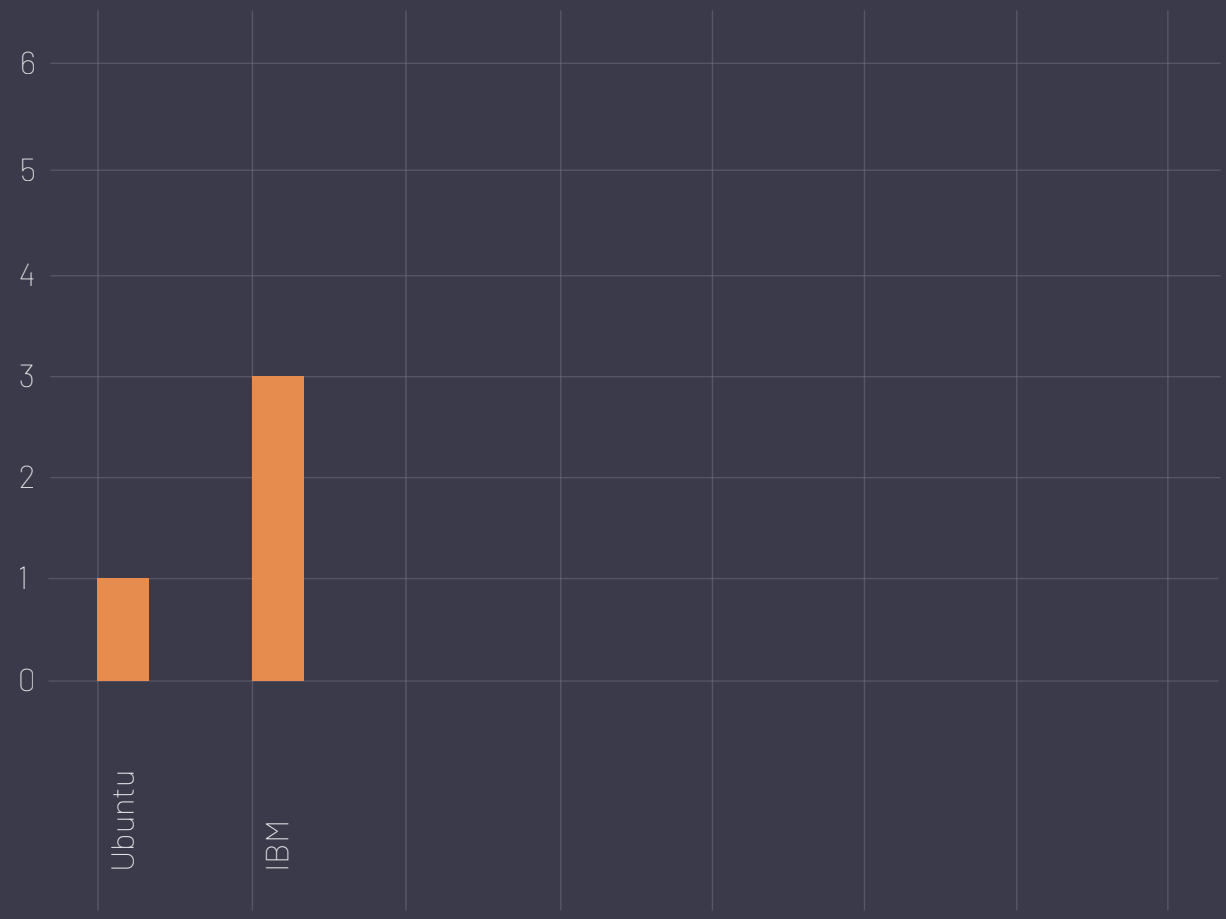
This graph present total released vulnerabilities including Zero-day vulnerability and EOS/EOL with their count.



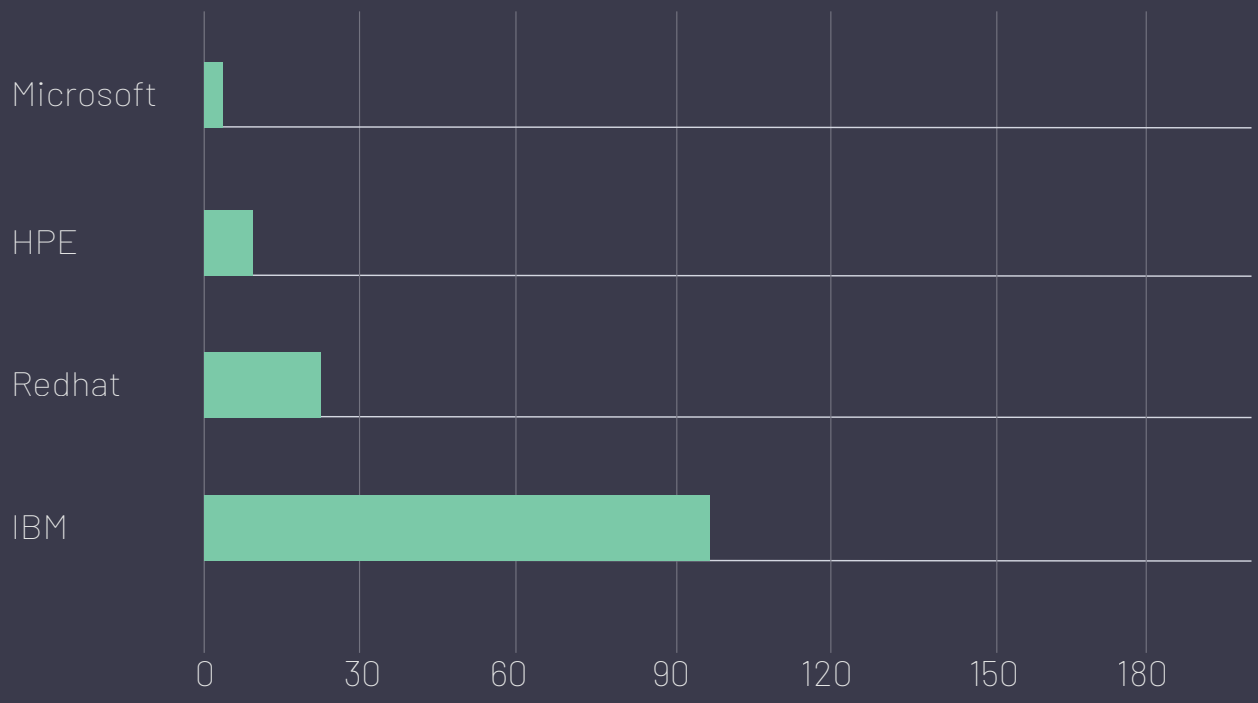
Product wise Released EOS/EOL count



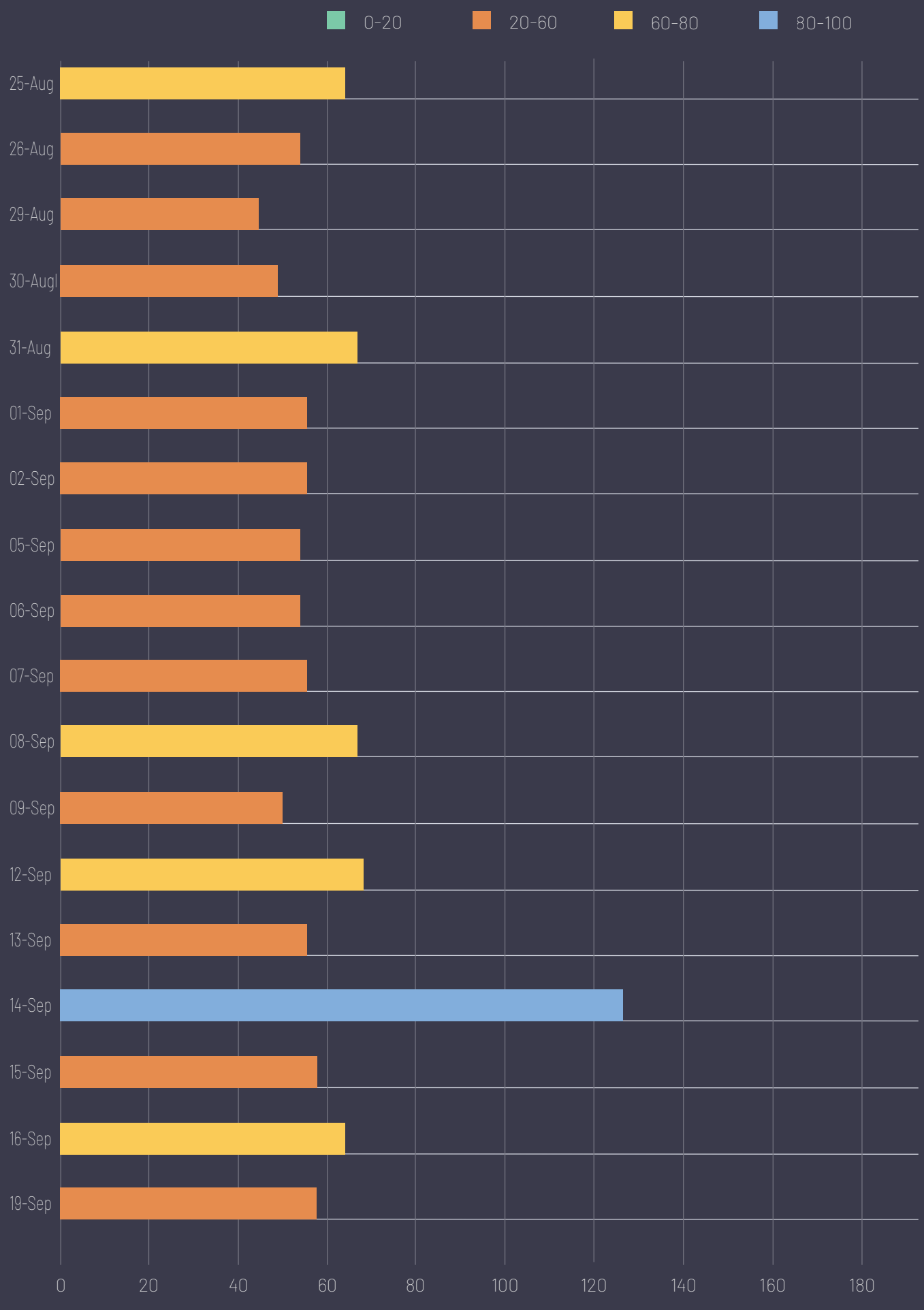
Product wise Released Non-CVE ID or Zero Day vulnerabilities Count

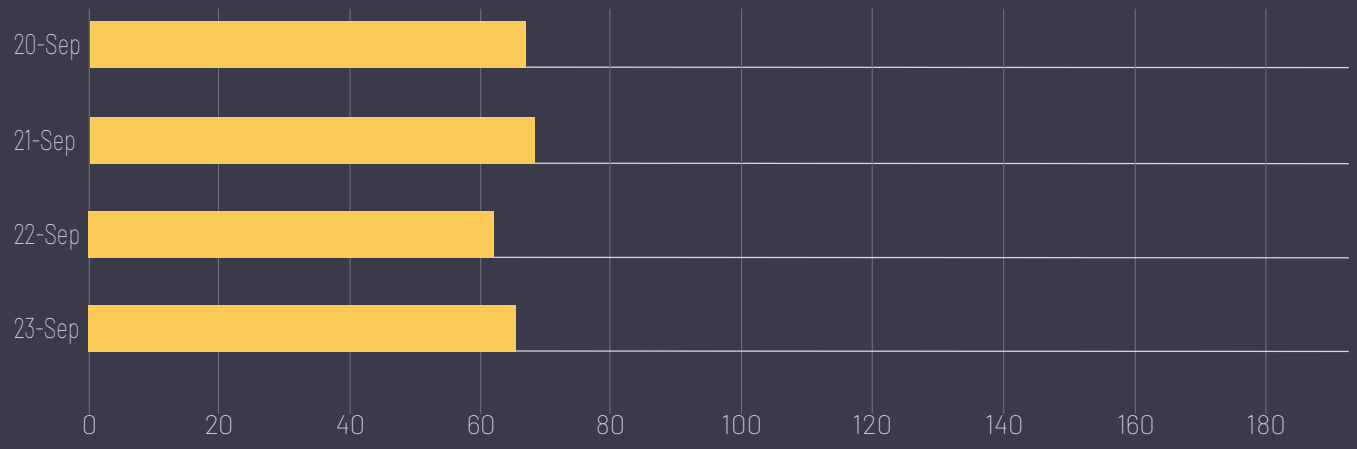


Critical CVE count

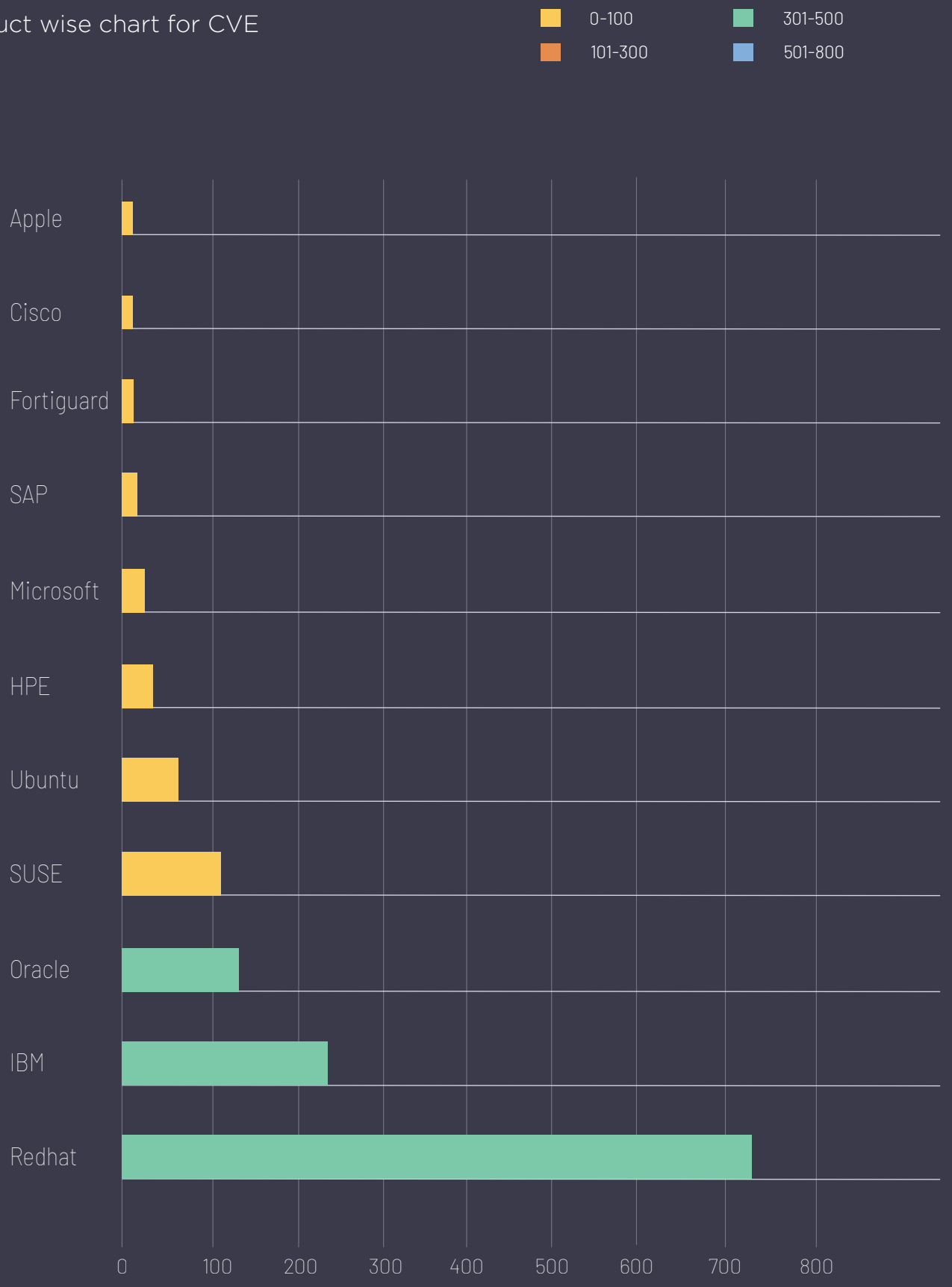


Datewise Releasd Vulnerabilities Count, Fortnightly Summarized





Product wise chart for CVE



TOP VULNERABILITIES OF THE WEEK

Data	CVE ID	Vendor	Product	Summary	Recommendation
29-08-22	CVE-2022-27782 CVE-2022-27774 CVE-2022-22576 CVE-2022-27776 CVE-2022-23267 CVE-2022-29117 CVE-2022-29145 CVE-2021-3737 CVE-2021-4189 CVE-2021-3634	IBM	IBM Robotic Process Automation for Cloud Pak 21.0.1, 21.0.2	Multiple vulnerabilities may affect IBM Robotic Process Automation for Cloud Pak	Updates are available please see below reference link: https://www.ibm.com/blogs/psirt/security-bulletin-multiple-vulnerabilities-may-affect-ibm-robotic-process-automation-for-cloud-pak/
30-08-22	CVE-2020-14039 CVE-2020-15586 CVE-2020-16845 CVE-2020-24553 CVE-2020-28362 CVE-2020-28366 CVE-2020-28367 CVE-2020-7919 CVE-2021-27918 CVE-2021-29923 CVE-2021-3114 CVE-2021-31525	IBM	IBM Robotic Process Automation for Cloud Pak 21.0.1, 21.0.2, 21.0.3	Multiple Security Vulnerabilities may affect IBM Robotic Process Automation for Cloud Pak	Updates are available please see below reference link: https://www.ibm.com/blogs/psirt/security-bulletin-multiple-security- vulnerabilities-may-affect-ibm-robotic-process-automation-for-cloud-pak-4/
31-08-22	CVE-2020-4301 CVE-2021-3749 CVE-2020-36518 CVE-2022-29078 CVE-2021-29418 CVE-2021-28918 CVE-2021-39009 CVE-2020-28469 CVE-2021-39045 CVE-2021-43797 CVE-2021-44533	IBM	IBM Cognos Analytics 11.2.x IBM Cognos Analytics 11.1.x	IBM Cognos Analytics has addressed multiple vulnerabilities	Updates are available please see below reference link: https://www.ibm.com/blogs/psirt/security-bulletin-ibm-cognos-analytics-has-addressed-multiple-vulnerabilities-9/

Data	CVE ID	Vendor	Product	Summary	Recommendation
08-09-22	CVE-2021-23450	IBM	IBM Business Automation Workflow containersV22.0.1 V21.0.3 – V21.0.3-IF010 V21.0.2 all fixes V20.0.0.2 all fixes V20.0.0.1 all fixes IBM Business Automation Workflow traditionalV22.0.1 V21.0.1 – V21.0.3 V20.0.0.1 – V20.0.0.2 V19.0.0.1 – V19.0.0.3 V18.0.0.0 – V18.0.0.2 IBM Business Process ManagerV8.6.0.0 – V8.6.0.201803 V8.5.0.0 – V8.5.0.201706	Prototype pollution vulnerability affect IBM Business Automation Workflow and IBM Business Process Manager	Updates are available please see below reference link: https://www.ibm.com/blogs/psirt/security-bulletin-prototype-pollution- vulnerability-affect-ibm-business-automation-workflow-and-ibm-business-process-manager-bpm-cve-2021-23450/
09-09-22	CVE-2022-24785 CVE-2018-1000613 CVE-2020-15522 CVE-2020-26939 CVE-2022-22968 CVE-2017-18214 CVE-2016-4055 CVE-2022-22314 CVE-2018-1000180	IBM	IBM Planning Analytics Workspace 2.0	IBM Planning Analytics Workspace is affected by multiple vulnerabilities	Updates are available please see below reference link: https://www.ibm.com/blogs/psirt/security-bulletin-ibm-planning-analytics-workspace-is-affected-by-multiple-vulnerabilities-cve-2022-22968-cve-2022-24785-cve-2017-18214-cve-2016-4055-cve-2018-1000613-cve-2020-15522- cve-2018-1/
12-09-22	CVE-2022-1292 CVE-2022-1586 CVE-2022-2068 CVE-2022-2097 CVE-2022-2526 CVE-2022-29154 CVE-2022-31129 CVE-2022-32206 CVE-2022-32208 CVE-2022-36067	Redhat	multicluster engine for Kubernetes Text-only Advisories x86_64	Multicluster Engine for Kubernetes 2.0.2 security and bug fixes	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2022:6422
14-09-22	CVE-2022-1012 CVE-2022-1292 CVE-2022-1586 CVE-2022-1785 CVE-2022-1897 CVE-2022-1927 CVE-2022-2068 CVE-2022-2097 CVE-2022-2526 CVE-2022-29154 CVE-2022-31129 CVE-2022-32206 CVE-2022-32208	Redhat	Red Hat Advanced Cluster Management for Kubernetes 2 for RHEL 8 x86_64	Red Hat Advanced Cluster Management 2.5.2 security fixes and bug fixes	Updates are available please see below reference link: https://access.redhat.com/errata/RHSA-2022:6507

Data	CVE ID	Vendor	Product	Summary	Recommendation
16-09-22	CVE-2022-28627 CVE-2022-28628 CVE-2022-28631 CVE-2022-28632	HPE	HPE Integrated Lights-Out 5 (iLO 5)	HPE Integrated Lights-Out 5 (iLO 5), Multiple Vulnerabilities	Updates are available please see below reference link: https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04333en_us
19-09-22	CVE-2022-34718	Microsoft	Windows 10 for 32-bit Systems Windows 10 for x64-based Systems Windows 10 Version 1607 for 32-bit Systems Windows 10 Version 1607 for x64-based Systems Windows 10 Version 1809 for 32-bit Systems Windows 10 Version 1809 for ARM64-based Systems Windows 10 Version 1809 for x64-based Systems Windows 10 Version 20H2 for 32-bit Systems Windows 10 Version 20H2 for ARM64-based Systems Windows 10 Version 20H2 for x64-based	Windows TCP/IP Remote Code Execution Vulnerability	Updates are available please see below reference link: https://msrc.microsoft-.com/update-guide/vulnerability/CVE-2022-34718
21-09-22	CVE-2022-27774 CVE-2021-22947 CVE-2021-22945 CVE-2021-22946 CVE-2022-22576 CVE-2022-32206 CVE-2022-32207 CVE-2022-32208 CVE-2022-32205 CVE-2022-27775 CVE-2022-27781 CVE-2022-27782 CVE-2022-27776	IBM	IBM Spectrum Protect Plus 10.1.0-10.1.11	Vulnerabilities in libcurl affect IBM Spectrum Protect Plus SQL, File Indexing, and Windows Host agents	Updates are available please see below reference link: https://www.ibm.com/blogs/psirt/security-bulletin-vulnerabilities-in-libcurl-affect-ibm-spectrum-protect-plus-sql-file-indexing-and-windows-host-agents/

Global Presence

USA / Sattrix Information Security Incorportation
UK/ EU / Sattrix Info Security Ltd
MEA / Sattrix Information Security DMCC
India / Sattrix Information Security (P) Ltd

Office Address
1 Parklane Blvd, Ste 729 E;
Dearborn, MI 48126

Golbal SOC
516, 517 Shivalik Shilp,
Iscon Cross Road, S G Highway, Ahmedabad

+1 416-917-8344 info sattrix.com www.sattrix.com