Gattrix

SECURITY INTELLIGENCE ADVISORY

25th July 2022 - 24th Aug 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

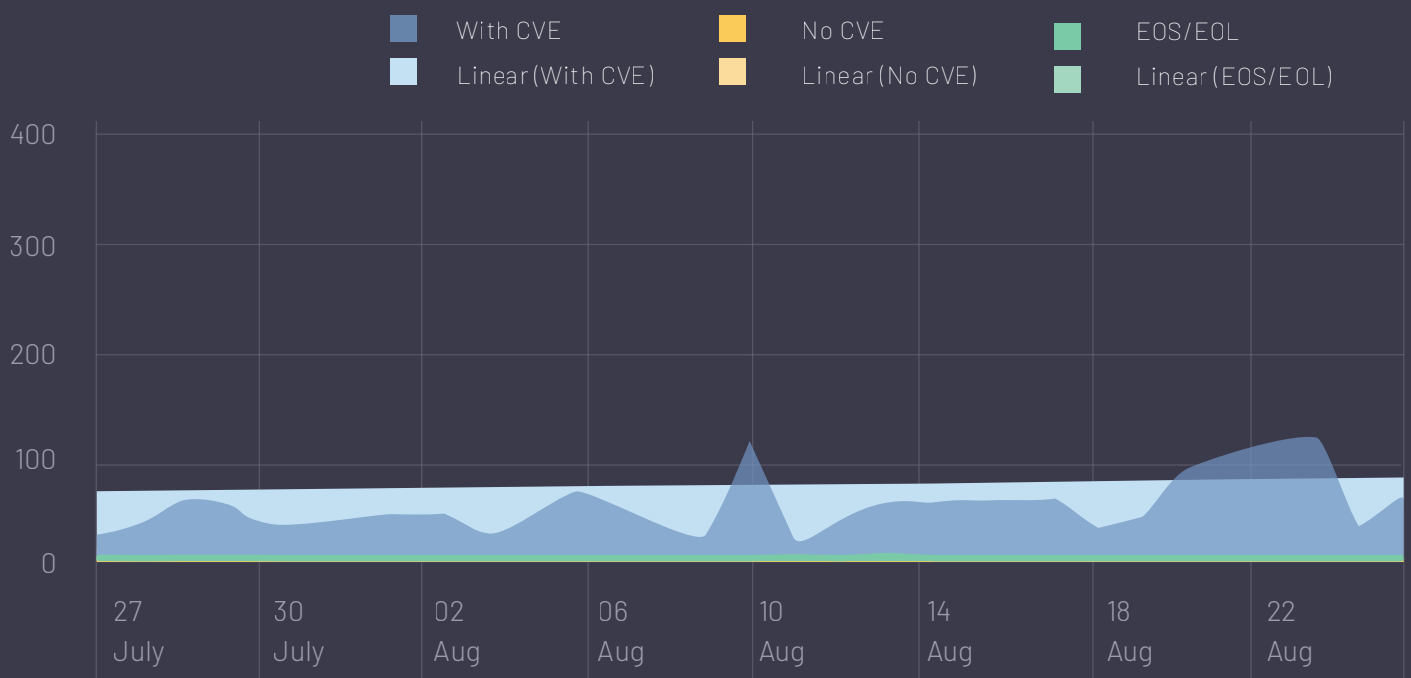
Every organization – large, medium and small has a huge risk and a typical challenge of managing vulnerabilities present in the operating systems, Vulnerabilities that are not attended possess a very high risk and can cost your organization various threats and damage. There is threat from users within 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.

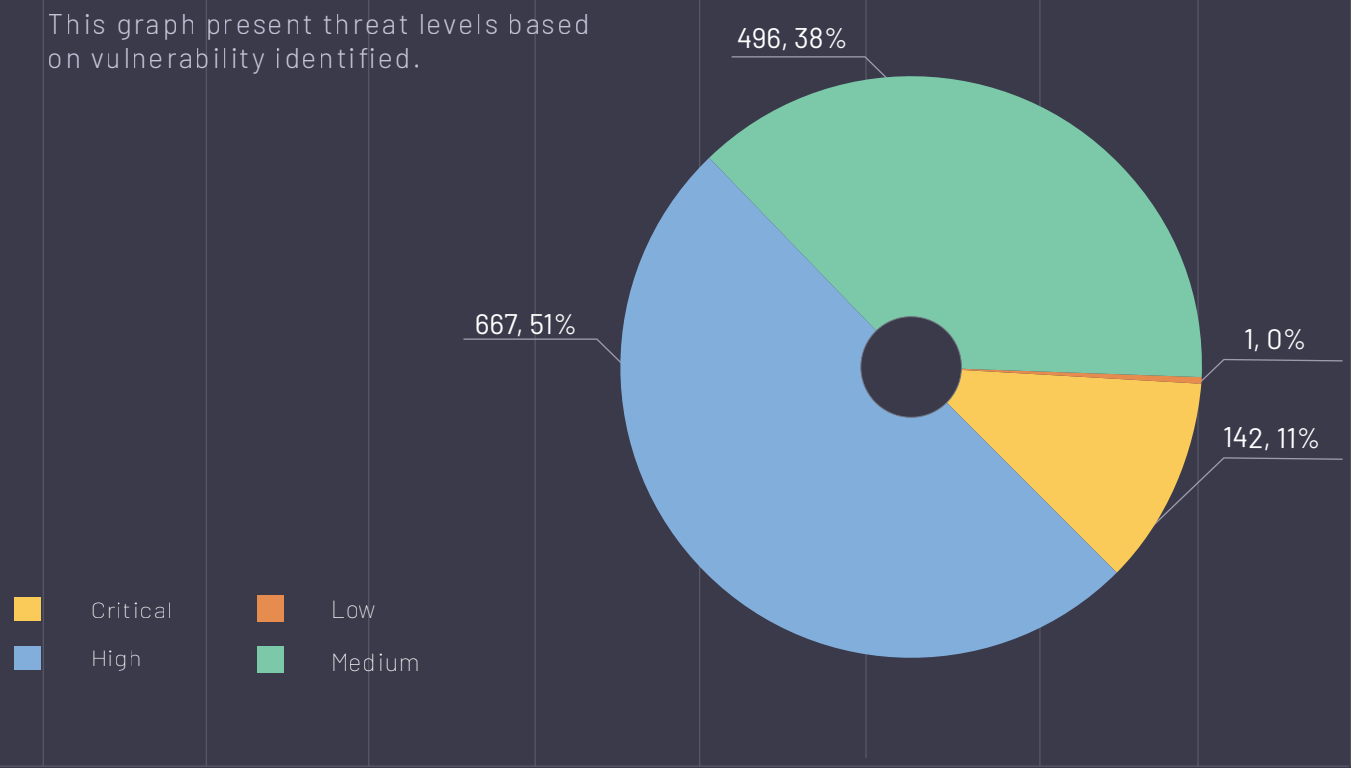
EXECUTIVE SUMMARY

Overall Monthly Vulnerability Trend Chart



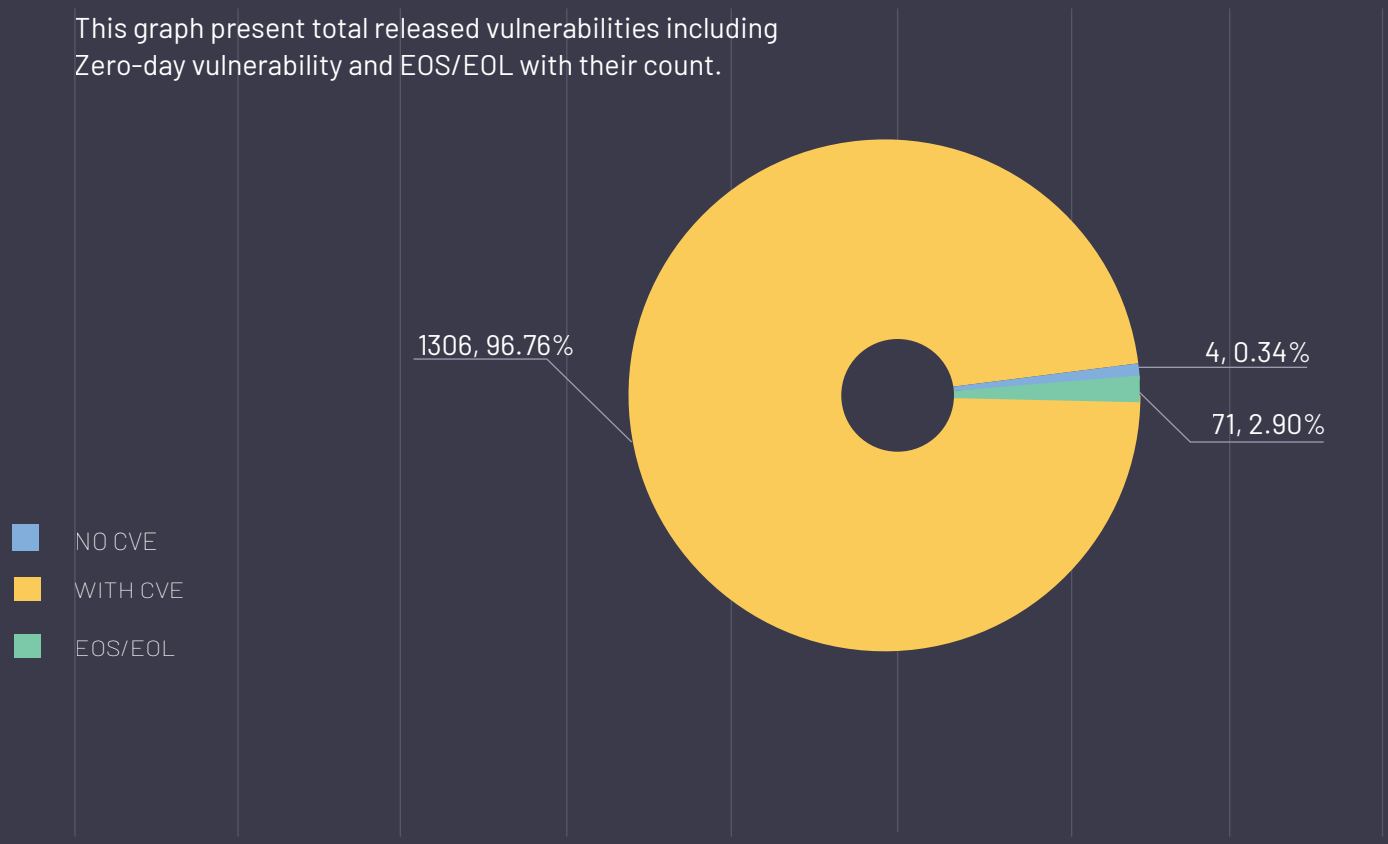
Released Vulnerabilities and severity wise count low severity count

This graph present threat levels based on vulnerability identified.

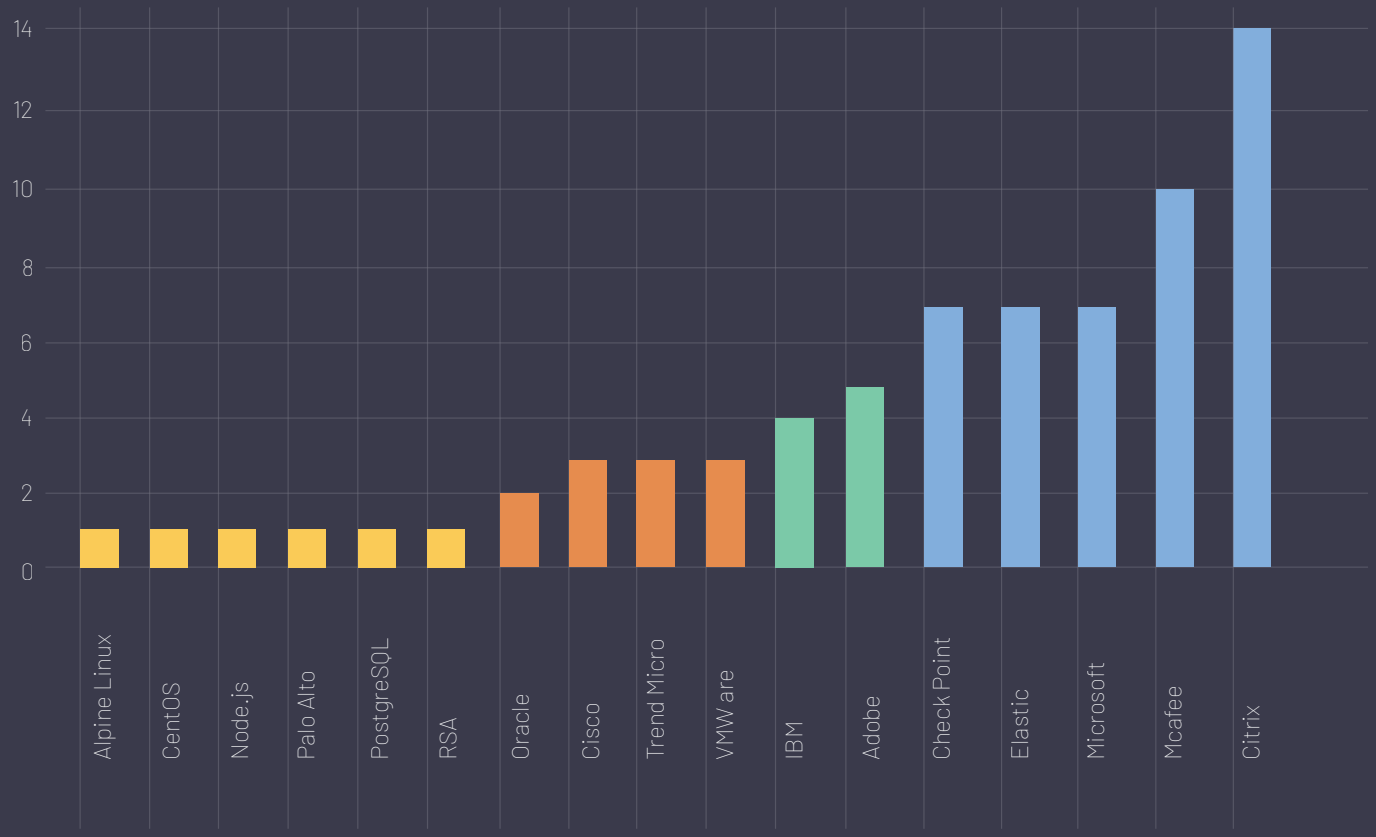


EXECUTIVE SUMMARY

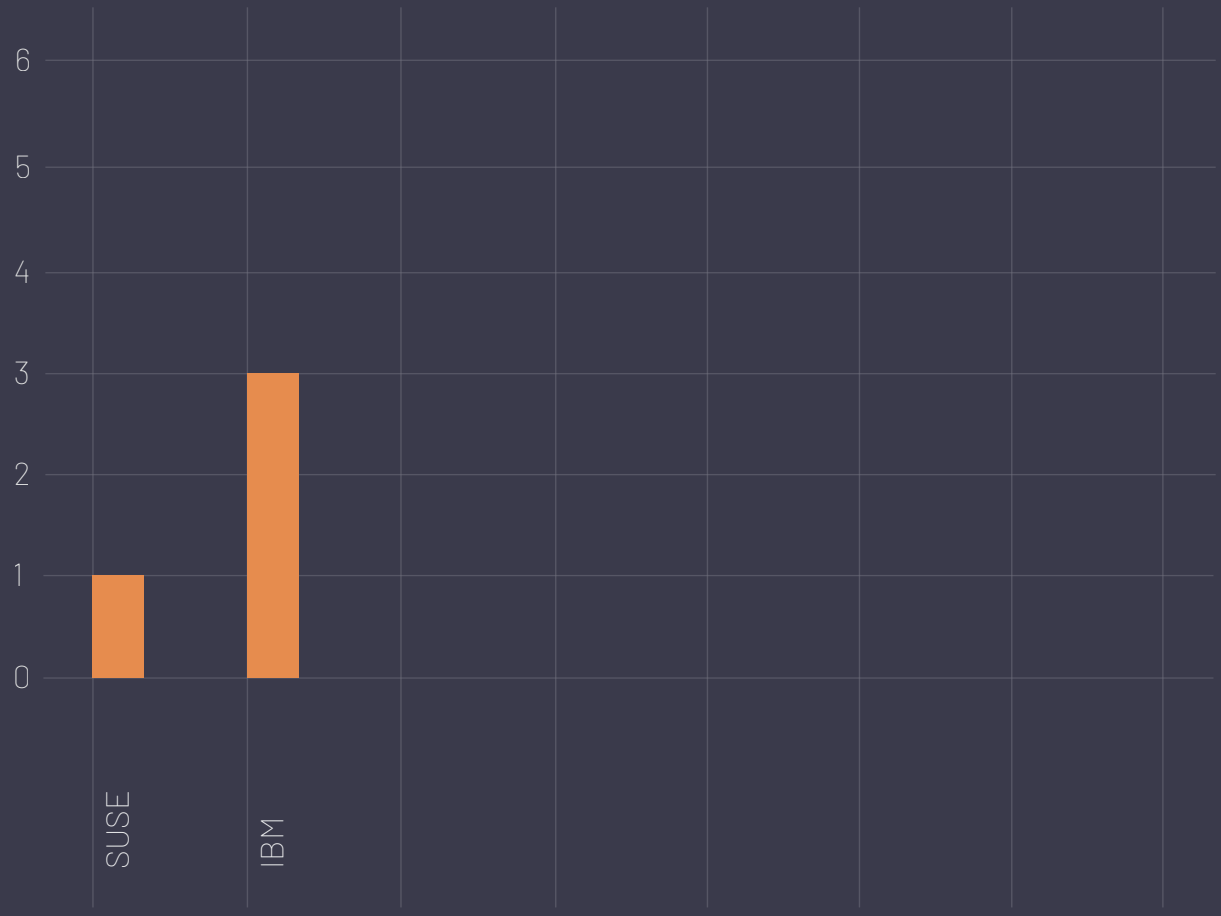
This graph present total released vulnerabilities including Zero-day vulnerability and EOS/EOL with their count.



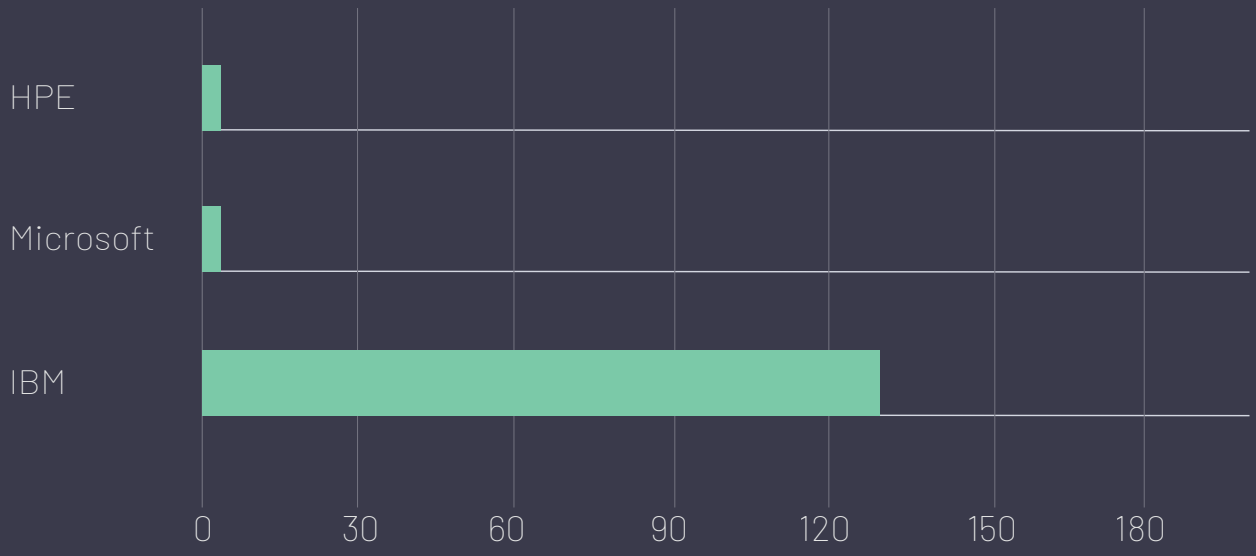
Product wise Released EOS/EOL count



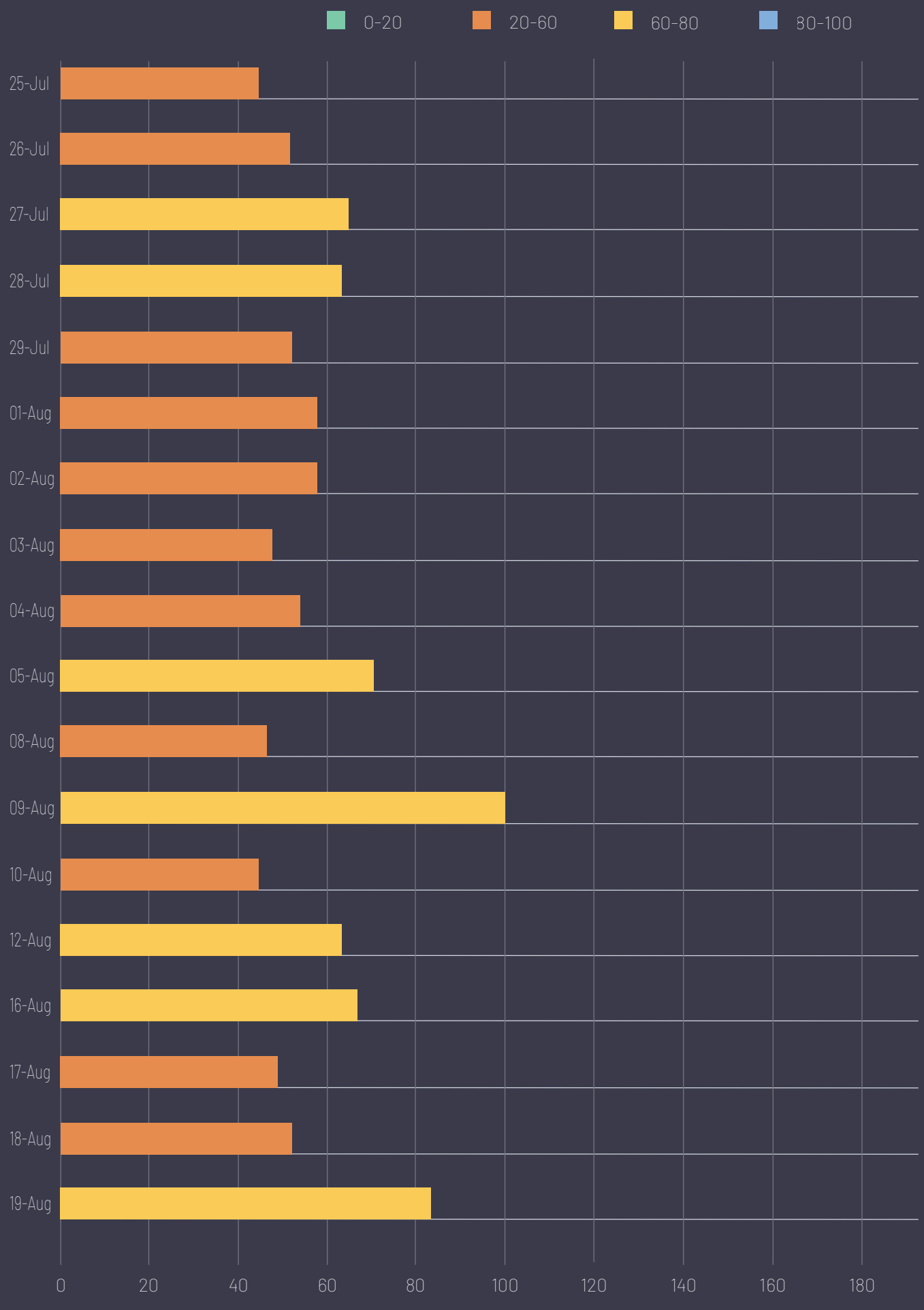
Product wise Released Non-CVE ID or Zero Day vulnerabilities Count

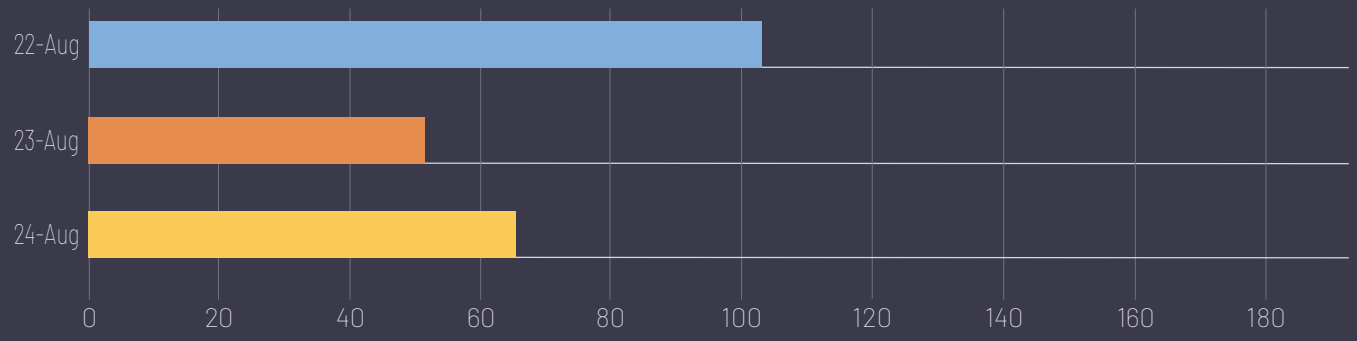


Critical CVE count

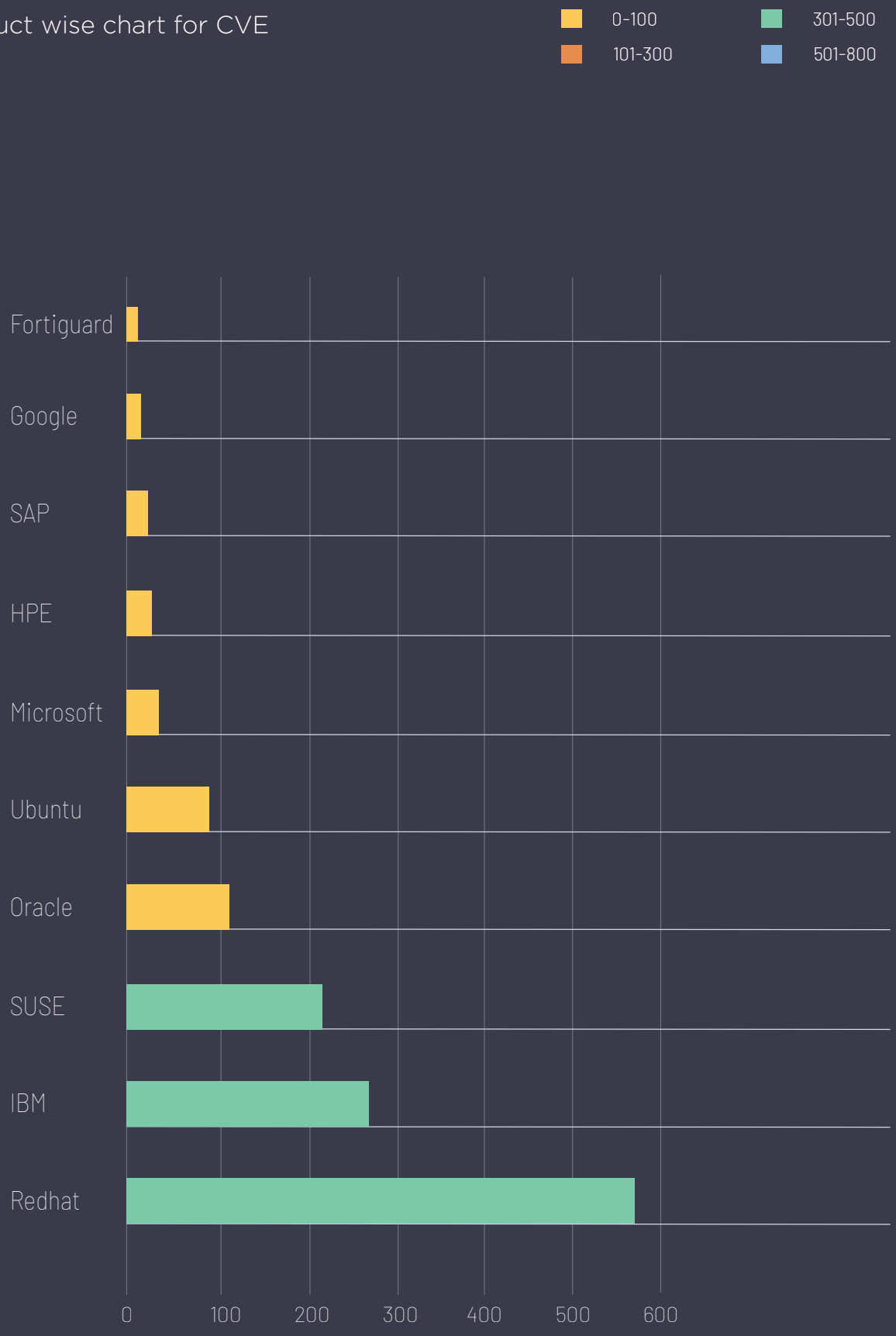


Datewise Releasd Vulnerabilities Count, Fortnightly Summarized





Product wise chart for CVE



TOP VULNERABILITIES OF THE WEEK

Data	CVE ID	Vendor	Product	Summary	Recommendation
27-07-22	CVE-2022-23218 CVE-2022-23219 CVE-2021-3999 CVE-2022-0261 CVE-2022-0359 CVE-2022-0392 CVE-2022-0361 CVE-2022-23308 CVE-2021-23177 CVE-2021-31566 CVE-2021-45960 CVE-2021-46143 CVE-2022-22822 CVE-2022-22823 CVE-2022-22824 CVE-2022-22825 CVE-2022-22826 CVE-2022-22827	IBM	IBM QRadar SIEM 7.3.0 – 7.3.3 Fix Pack 11 IBM QRadar SIEM 7.4.0 – 7.4.3 Fix Pack 5 IBM QRadar SIEM 7.5.0 – 7.5.0 Update Pack 1	IBM QRadar SIEM Application Framework Base Image is vulnerable to using components with Known Vulnerabilities	Updates are available please see below reference link: https://www.ibm.com/blogs/psirt/security-bulletin-ibm-qradar-siem-application-framework-base-image-is-vulnerable-to-using-components-with-known- vulnerabilities-2/
29-07-22	CVE-2022-28627 CVE-2022-28628 CVE-2022-28631 CVE-2022-28632	HPE	HPE Integrated Lights-Out 5 (iLO 5) for HPE Gen10 Servers - Prior to 2.71 HPE Apollo 2000 Gen10 Plus System - Prior to 2.71 HPE Apollo 4200 Gen10 Plus System - Prior to 2.71 HPE Apollo 4200 Gen10 Server - Prior to 2.71 - HPE ProLiant XL420 Gen10 Server HPE Apollo 4510 Gen10 System - Prior to 2.71 HPE Apollo 6500 Gen10 Plus System - Prior to 2.71	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
04-08-22	CVE-2022-1552 CVE-2022-22969 CVE-2022-21496 CVE-2022-21434 CVE-2022-21443 CVE-2022-22971 CVE-2021-45346 CVE-2022-24785 CVE-2021-35561 CVE-2022-0492 CVE-2022-22970	IBM	IBM DRM 2.0.6.13	IBM Data Risk Manager is affected by multiple vulnerabilities including remote code execution in Apache Log4j 1.x	Updates are available please see below reference link: https://www.ibm.com/blogs/psirt/security-bulletin-ibm-data-risk-manager-is- affected-by-multiple-vulnerabilities-including-remote-code-execution-in-apache-log4j-1-x/

Data	CVE ID	Vendor	Product	Summary	Recommendation
12-08-22	CVE-2022-24921 CVE-2022-27782 CVE-2022-27776 CVE-2022-29824 CVE-2022-27774 CVE-2022-22576 CVE-2022-25313 CVE-2022-25314 CVE-2022-28327 CVE-2022-24675 CVE-2022-22393 CVE-2022-22475 CVE-2022-29526 CVE-2021-40528	IBM	IBM MQ Operato-rEUS release 1.3.5 and LTS Release 2.0.0 IBM supplied MQ Advanced container imagesv9.2.0.5-r3 and v9.3.0.0-r1	IBM MQ Operator and Queue manager container images are vulnerable to multiple vulnerabilities from Golang Go, libxml2, curl, expat, libgcrypt and IBM WebSphere Application Server Liberty	Updates are available please see below reference link: https://www.ibm.com/blogs/p-sirt/security-bulle-tin-ibm-mq-oper-ator-and-queue- manag-er-container-images-are-vul-nerable-to-multiple-vulnerabi-lities-from- golang-go-libx-ml2-curl-expat-libg-crypt-and-ibm-websphere-ap-plication-server- li/
16-08-22	CVE-2022-34696	Microsoft	Windows Server 2012 R2 (Server Core installation) Windows Server 2012 R2 Windows 8.1 for x64based systems Windows Server 2016 (Server Core installation) Windows Server 2016 Windows 10 Version 1607 for x64based Systems Windows 10 for x64based Systems Windows 10 Version 21H2 for x64based	Windows Hyper-V Remote Code Execution Vulnerability	Updates are available please see below reference link: https://msrc.microsoft-.com/update-guide/vulnera-bility/CVE-2022-34696
24-08-22	CVE-2021-43859 CVE-2022-24407 CVE-2021-22060 CVE-2021-3677 CVE-2022-22720 CVE-2021-28169 CVE-2021-34428 CVE-2021-28163 CVE-2021-28164 CVE-2021-34429 CVE-2021-28165 CVE-2021-45960 CVE-2021-46143	IBM	IBM QRadar SIEM 7.3.0 – 7.3.3 Fix Pack 11 IBM QRadar SIEM 7.4.0 – 7.4.3 Fix Pack 5 IBM QRadar SIEM 7.5.0 – 7.5.0 Update Pack 1	IBM QRadar SIEM includes components with multiple known vulnerabilities	Updates are available please see below reference link: https://ww-w.ibm.com/blogs/psirt/secu-rity-bulletin-ibm-qra-dar-siem-includes- compo-nents-with-multi-ple-known-vulnerabilities/

Global Presence

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

HQ
28, Damubhai colony,
Anjali cross roads, Bhattha, Ahmedabad – 007

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

+91 796 819 6800 info@sattrix.com www.sattrix.com