Sattrix®

SECURITY INTELLIGENCE ADVISORY

25th Nov 2020 - 24th Dec2020

www.sattrix.com

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

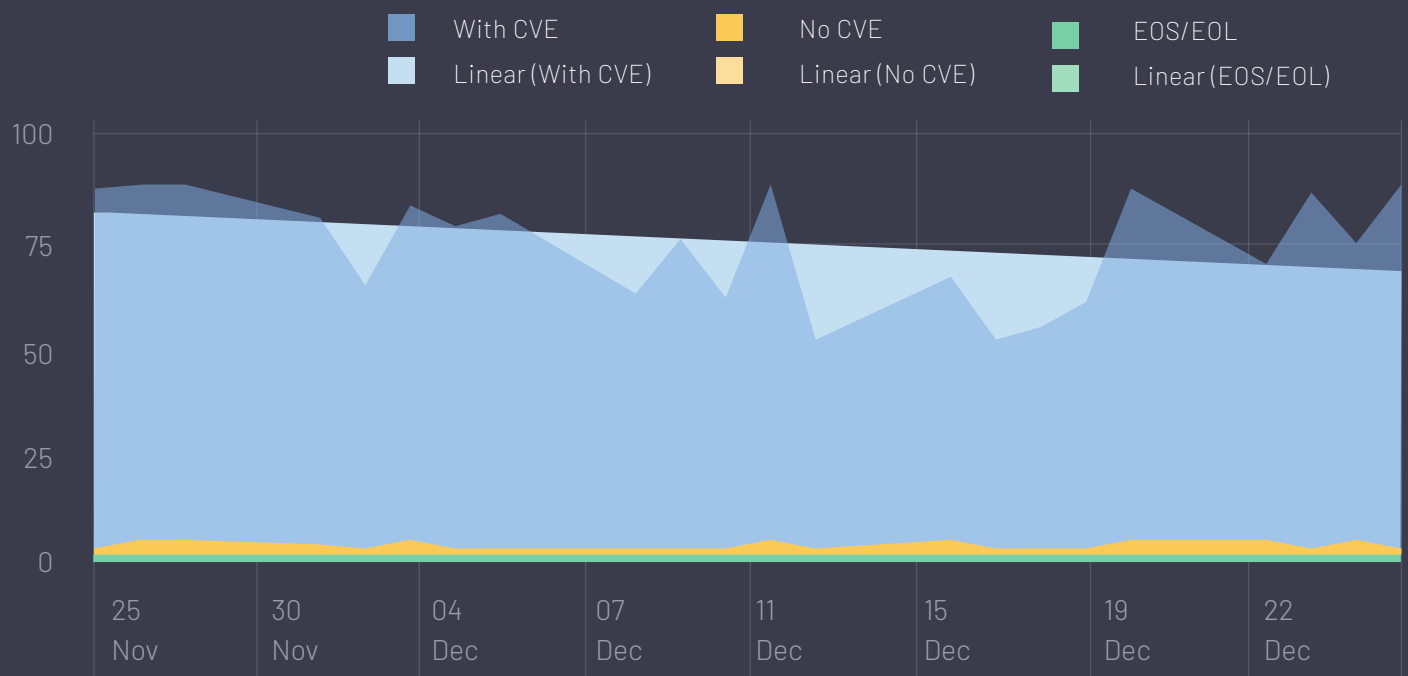
Every organization – large, medium and small has a huge risk and a typical challenge of managing vulnerabilities present in the operating systems, Vulnerabilities that are not attended possess a very high risk and can cost your organization various threats and damage. There is threat from users within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

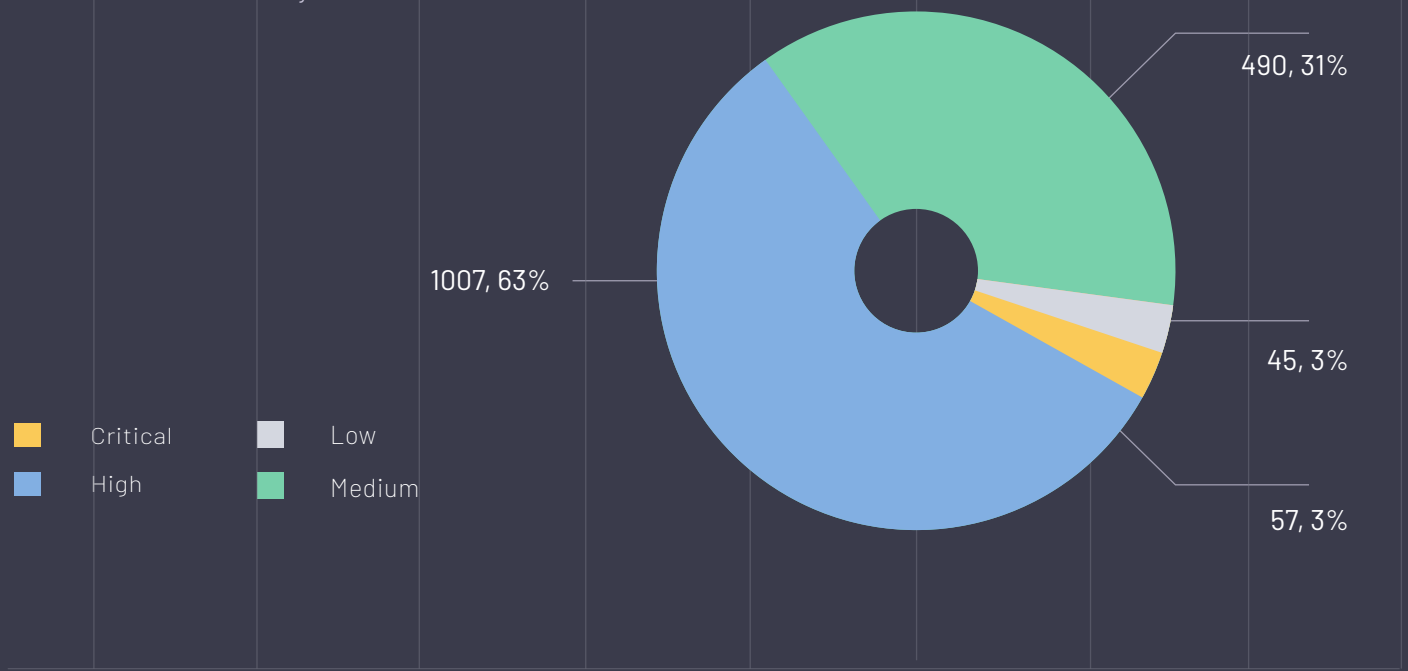
EXECUTIVE SUMMARY

Overall Monthly Vulnerability Trend Chart



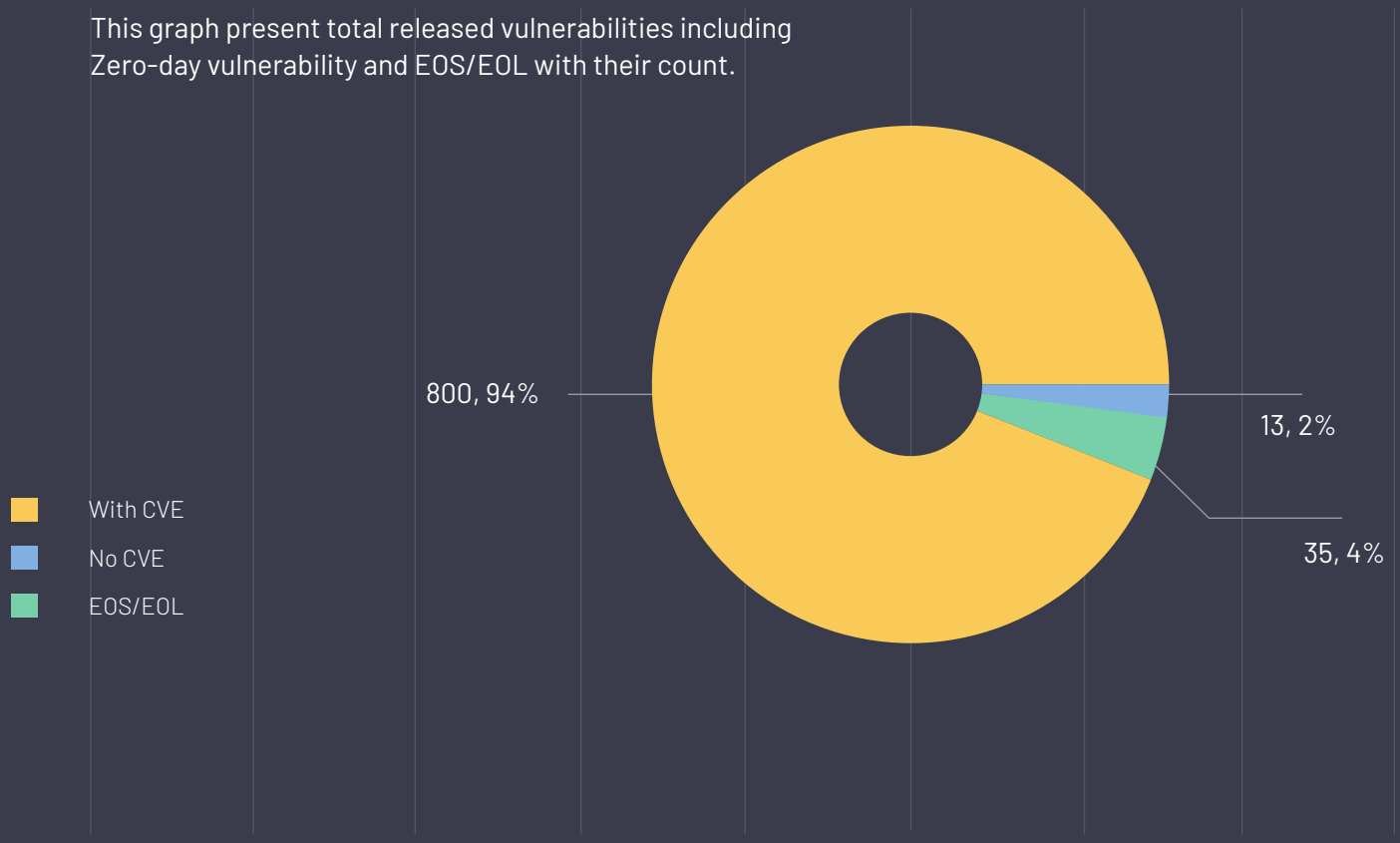
Released Vulnerabilities and severity wise count

This graph present threat levels based on vulnerability identified.

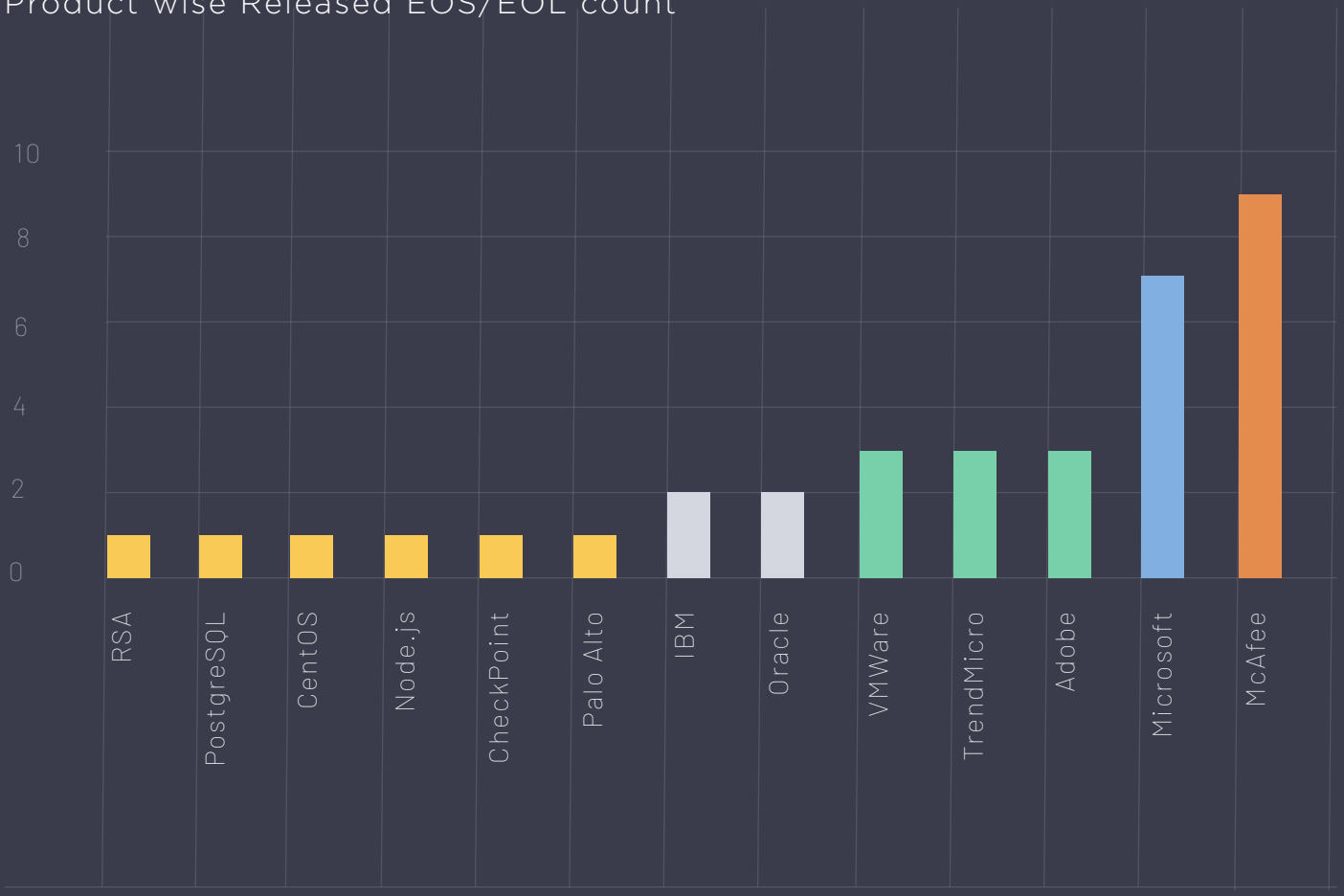


EXECUTIVE SUMMARY

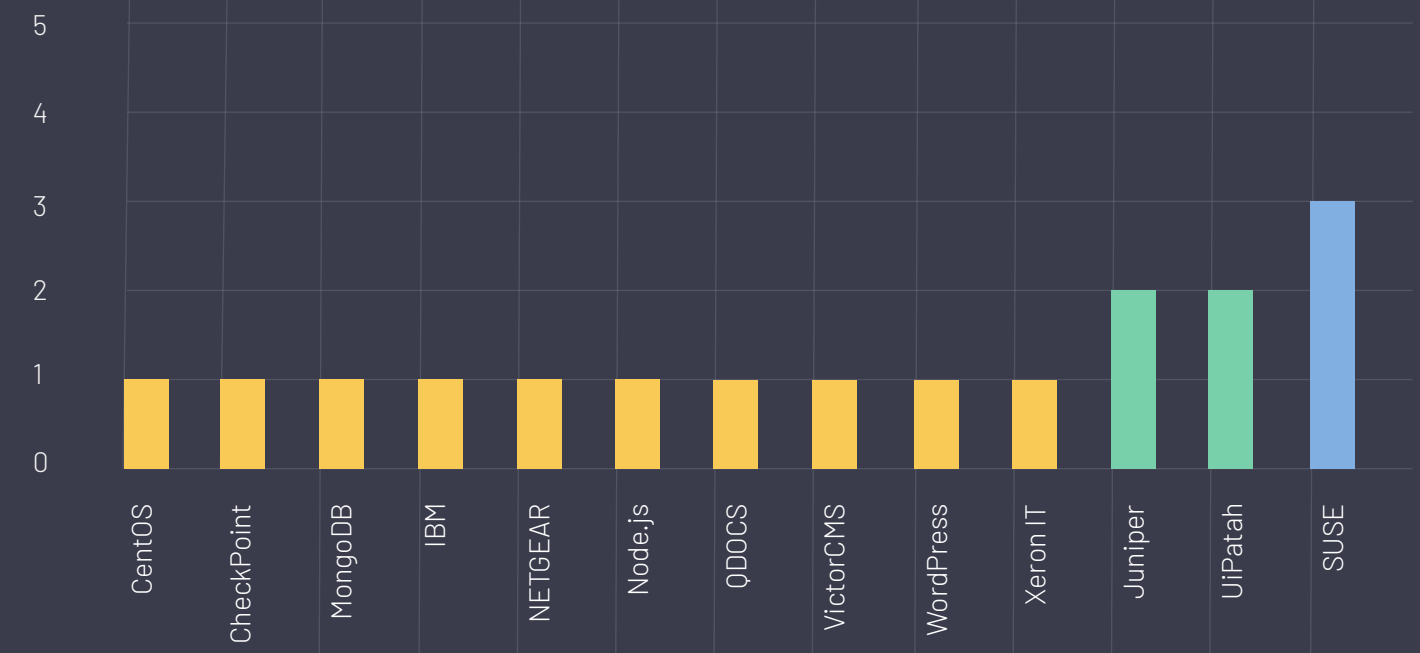
This graph present total released vulnerabilities including Zero-day vulnerability and EOS/EOL with their count.



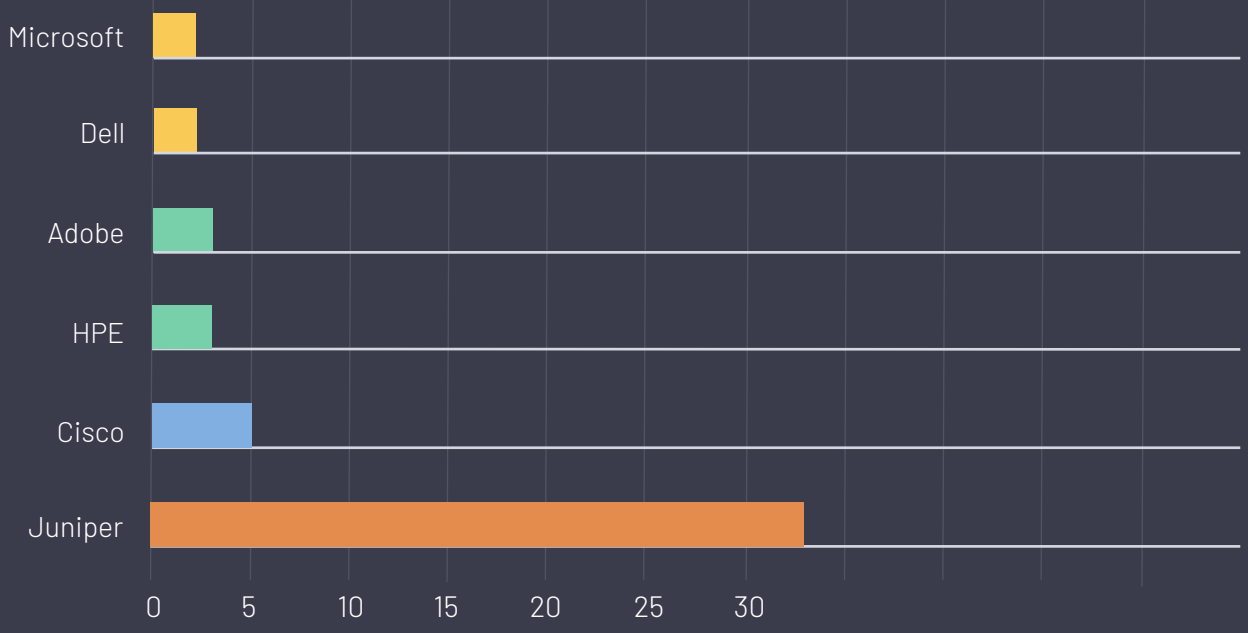
Product wise Released EOS/EOL count



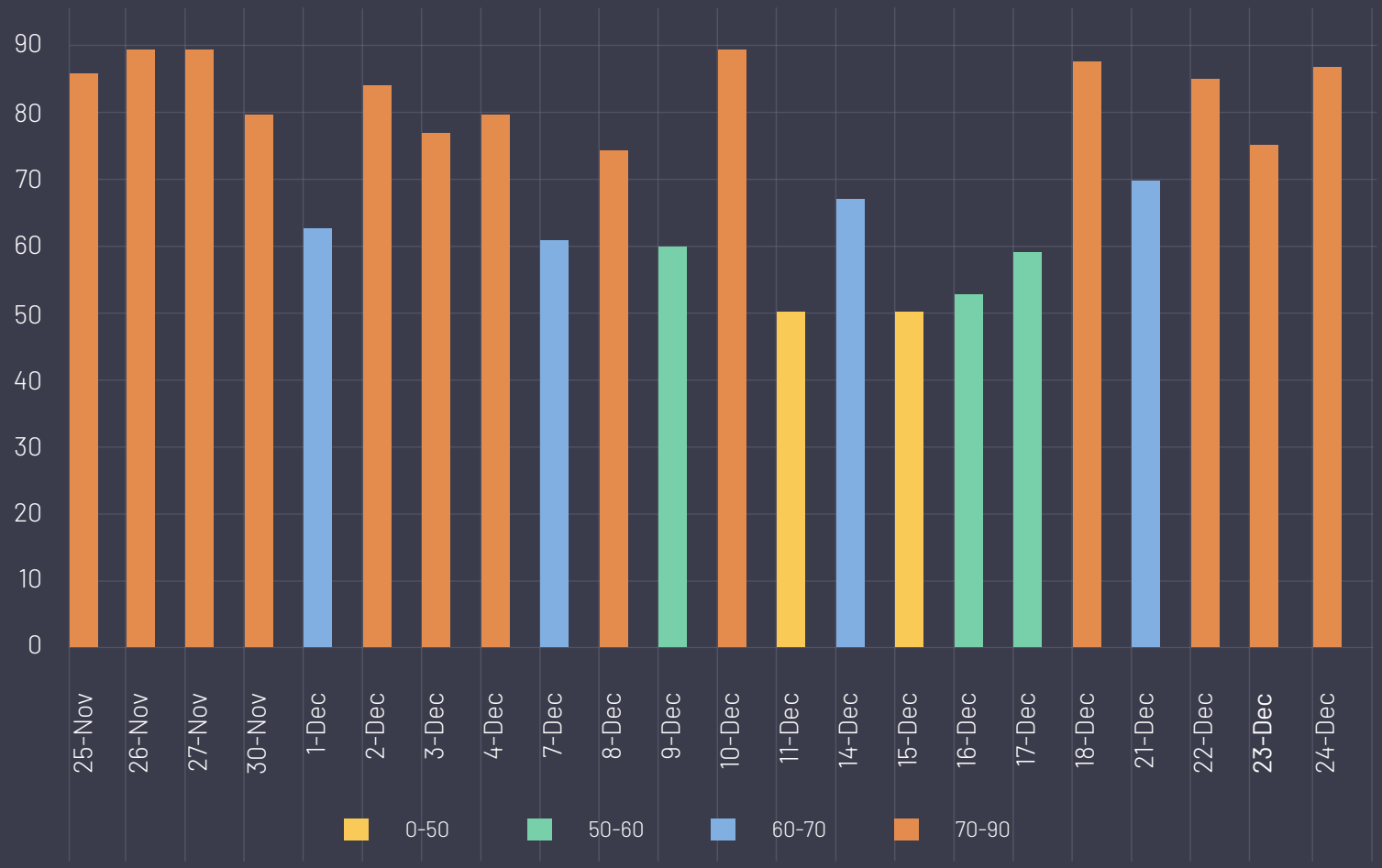
Product wise Released Non-CVE ID or Zero Day vulnerabilities count



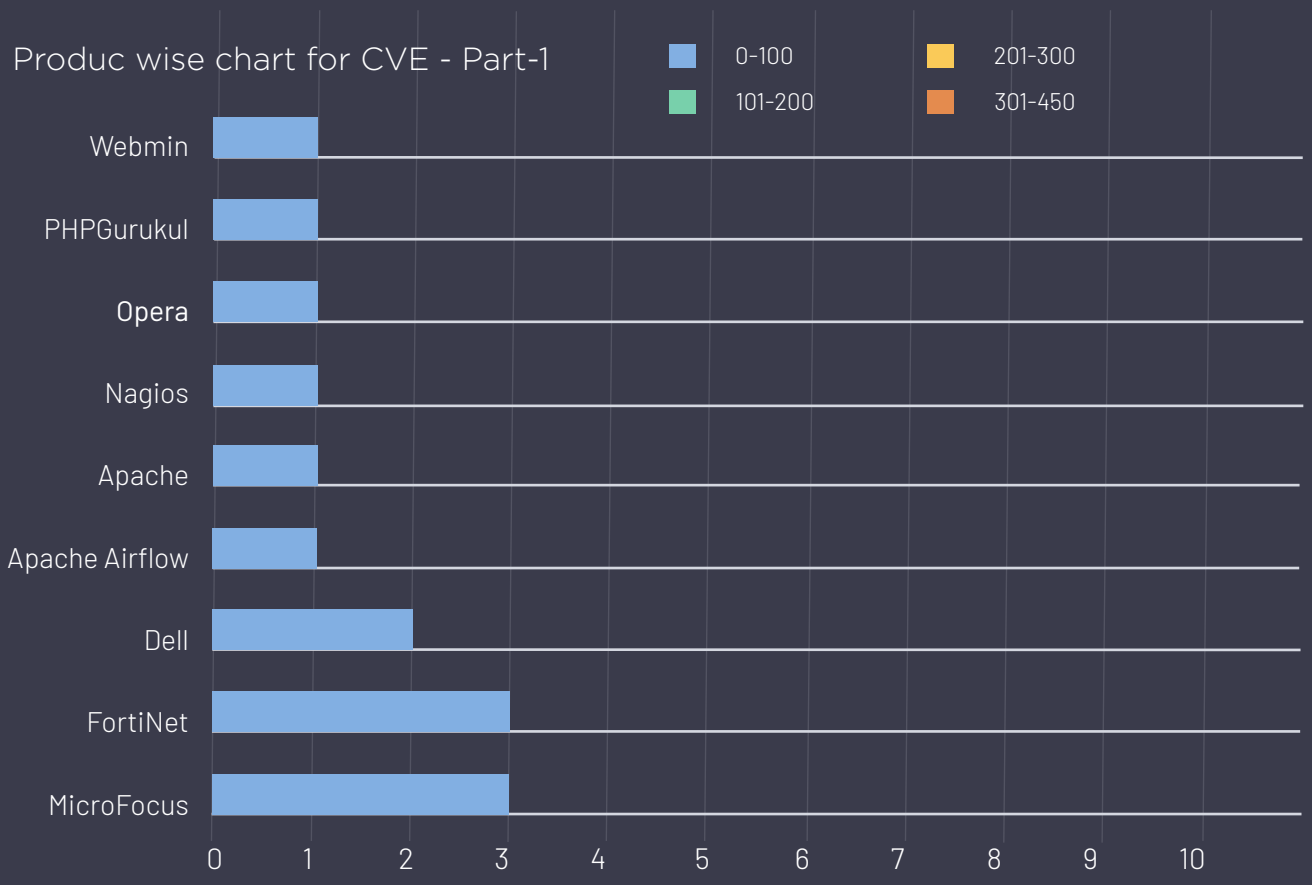
Critical CVE Count



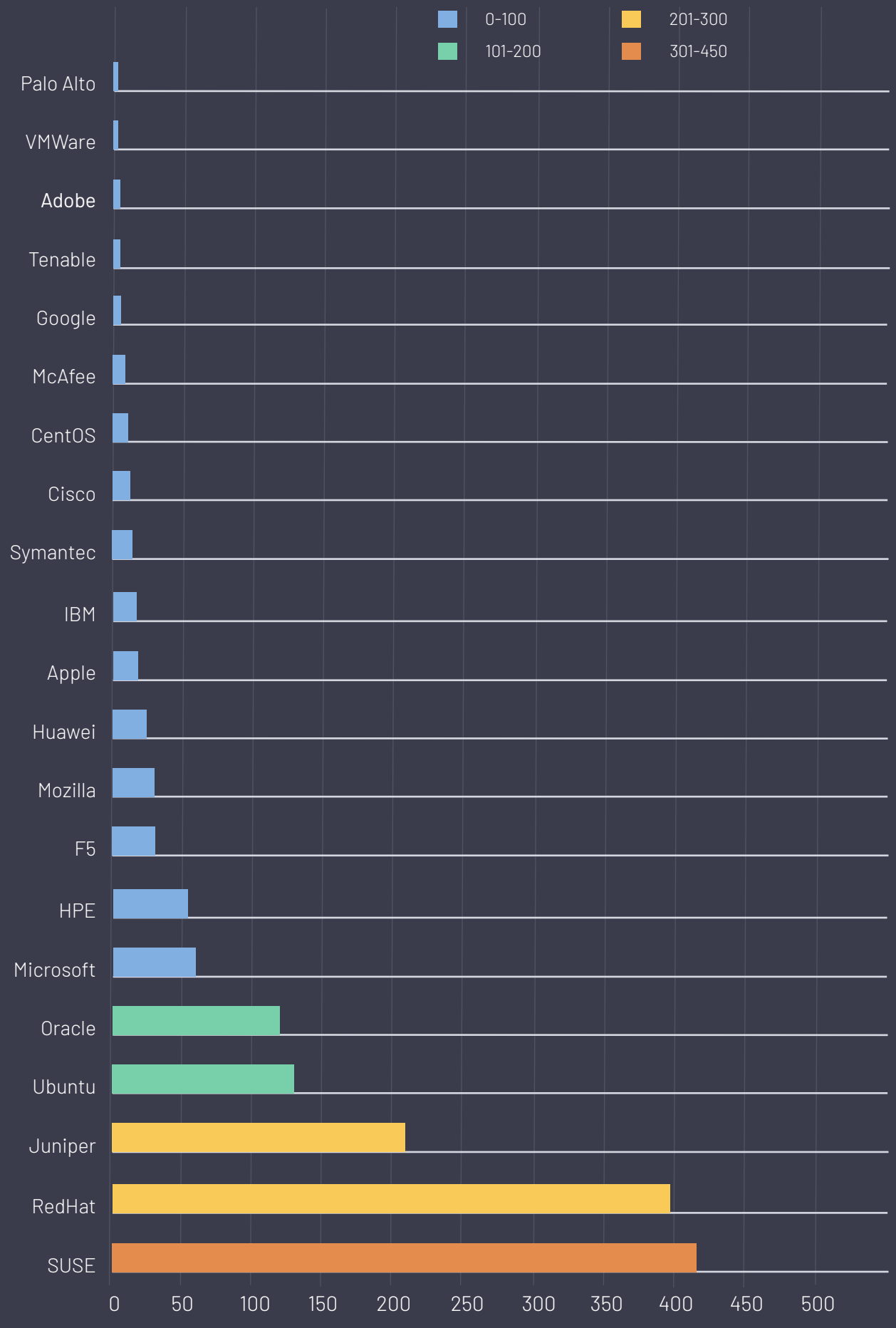
Date wise Released Vulnerabilities Count, fortnightly summarized



Produc wise chart for CVE - Part-1



Produc wise chart for CVE - Part-2



TOP VULNERABILITIES OF THE WEEK

Data	CVE ID	Vendor	Product	Summary	Recommendation
12 / 1 / 2020	CVE-2018-10875, CVE-2019-10744, CVE-2019-3828, CVE-2019-9636, CVE-2017-18342, CVE-2015-5224, CVE-2015-5739, CVE-2015-5740, CVE-2016-4800, CVE-2017-15095, CVE-2017-7525, CVE-2017-7614, CVE-2017-7657, CVE-2017-7658, CVE-2017-8283, CVE-2017-8421, CVE-2018-1126, CVE-2018-11307, CVE-2018-12699, CVE-2018-14599, CVE-2018-14600, CVE-2018-14718, CVE-2018-14719, CVE-2018-14720, CVE-2018-14721, CVE-2018-15686, CVE-2018-15688	Juniper	Contrail Networking	Contrail Networking: Multiple Vulnerabilities have been resolved in Release 1910	Updates are available please see below reference link https://kb.juniper.net/InfoCenter/index?page=content&id=JSA10967&cat=SIRT_1&actp=LIST
12 / 2 / 2020	CVE-2019-10173	Juniper	Juniper Secure Analytics (JSA) 7.3.2, 7.3.3.	Multiple vulnerabilities have been resolved in the Juniper Secure Analytics (JSA) 7.3.2 Patch 5, and 7.3.3 Patch 1 FixPack 1 by fixing vulnerabilities in the Linux kernel in addition to other software	Updates are available please see below reference link https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11007&cat=SIRT_1&actp=LIST
12 / 3 / 2020	CVE-2020-7199	HPE	HPE Edgeline Infrastructure Management Software - Prior to 1.21	Security vulnerability has been identified in the HPE Edgeline Infrastructure Manager, also known as HPE Edgeline Infrastructure Management Software. The vulnerability could be remotely exploited to bypass remote authentication leading to execution of arbitrary commands, gaining privileged access, causing denial of service, & changing the configuration.	Updates are available please see below reference link https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04063en_us

Data	CVE ID	Vendor	Product	Summary	Recommendation
12 / 4 / 2020	CVE-2018-18311 CVE-2018-18312	HPE	HP-UX Perl Software E.5.28.0.A	Multiple security vulnerabilities have been identified in HPUX Perl E.5.28.0.A. These vulnerabilities may cause buffer overflows through the use of crafted regular expressions, invalid write operations, malformed bytecode intrusion injections, or a heap-based buffer overflow.	Updates are available please see below reference link https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbux04065en_us
12 / 8/ 2020	CVE-2020-24440	Adobe	Adobe Prelude - 9.0.1 and earlier versions	Adobe has released updates for Adobe Prelude for Windows and macOS.	Updates are available please see below reference link https://helpx.adobe.com/security/products/prelude/apsb20-70.html
12 / 8/ 2020	CVE-2020-24445	Adobe	AEM CS AEM 6.5.6.0 and earlier, AEM 6.4.8.2 and earlier AEM 6.3.3.8 and earlier	Adobe has released updates for Adobe Experience Manager(AEM) and the AEM Forms add-on package.	Updates are available please see below reference link https://helpx.adobe.com/security/products/experiencemanager/apsb20-72.html
12 / 10 / 2020	CVE-2020-26085 CVE-2020-27127 CVE-2020-27132 CVE-2020-27133 CVE-2020-27134	Cisco	Cisco Jabber for Windows - 12.9	Multiple vulnerabilities in Cisco Jabber for Windows, Jabber for MacOS, and Jabber for mobile platforms could allow an attacker to execute arbitrary programs on the underlying operating system (OS) with elevated privileges or gain access to sensitive information.	Updates are available please see below reference link https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-jabber-ZktzjpgO
12 / 11 / 2020	CVE-2020-24447	Adobe	Lightroom Classic - 10.0 & earlier versions	Adobe has released updates for Adobe Lightroom Classic for Windows and macOS.	Updates are available please see below reference link https://helpx.adobe.com/security/products/lightroom/apsb20-74.html
12 / 14 / 2020	CVE-2020-17118 CVE-2020-17121	Microsoft	Microsoft SharePoint Foundation 2013 Service Pack 1 Microsoft SharePoint Foundation 2010	Microsoft SharePoint Remote Code Execution Vulnerability	Updates are available please see below reference link https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-17118

Data	CVE ID	Vendor	Product	Summary	Recommendation
			Service Pack 2 Microsoft SharePoint Server 2019 Microsoft SharePoint Enterprise Server 2016		https://msrc.microsoft.com/updateguide/vulnerability/CVE-2020-17121
12 / 22 / 2020	CVE-2020-29492 CVE-2020-29491	Dell	Dell Wyse 3040 Thin Client (ENG), Dell Wyse 3040 Thin Client (ENG), Dell Wyse 3040 Thin Client (JPN), Dell Wyse 3040 Thin Client (JPN), Dell Wyse 3040 Thin Client with PCoIP (ENG), Dell Wyse 3040 Thin Client with PCoIP (ENG), Dell Wyse 3040 Thin Client with PCoIP (JPN), Dell Wyse 3040 Thin Client with PCoIP (JPN), Dell Wyse 5010 Thin Client (ENG), Dell Wyse 5010 Thin Client (ENG), Dell Wyse 5010 Thin Client (JPN), Dell Wyse 5010 Thin Client (JPN), Dell Wyse 5010 Thin Client with PCoIP (ENG), Dell Wyse 5010 Thin Client with PCoIP (JPN), Dell Wyse 5040 Thin Client (ENG), Dell Wyse 5040 Thin Client (ENG) Dell Wyse 5040 Thin Client (JPN)	Dell Wyse ThinOS 8.6 Security Update for Insecure Default Configuration Vulnerabilities	Refer to Dell DSA Identifier: DSA-2020-281 for patch, upgrade or suggested workaround information. See References. https://exchange.xforce.ibmcloud.com/vulnerabilities/193555 https://www.dell.com/support/kbdoc/en-in/000180768/dsa-2020-281

Global Presence

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

HQ
28, Damubhai Colony,
Bhattha Paldi, Ahmedabad - 007

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

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