Sattrix

6th Jan – 13th Jan 2020

+91 796 819 6800 | info@sattrix.com

HOW DO YOU FIND VULNERABILITIES?

ABOUT US

Organizations worldwide are under constant threats. Prying eyes below black hats are glued to monitors. Their fingers are slamming keyboards and hitting mouse buttons; desperately in the pursuit of that one little crack! They not only jeopardize the target's day to day operations but in some cases, even put sensitive information at stake.

OUR SERVICES

ASSESSMENT & ADVISORY

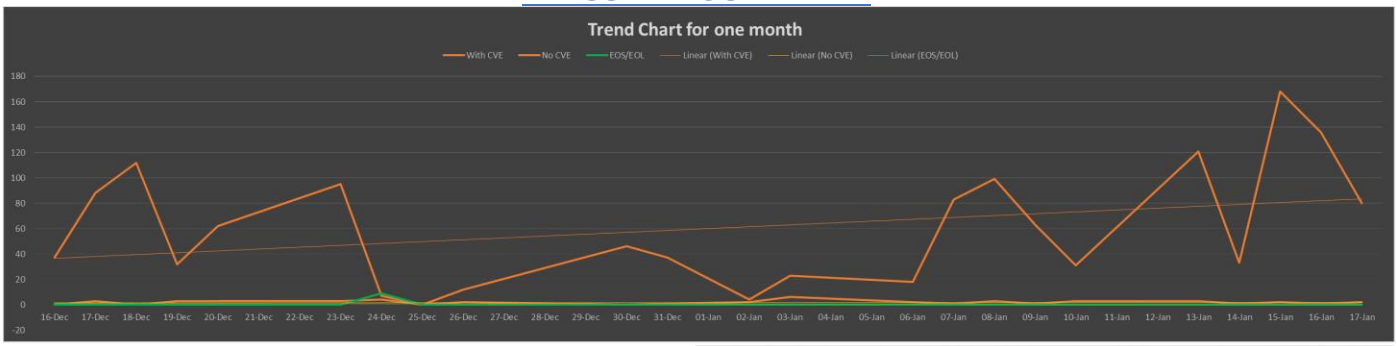
MANAGED SERVICES

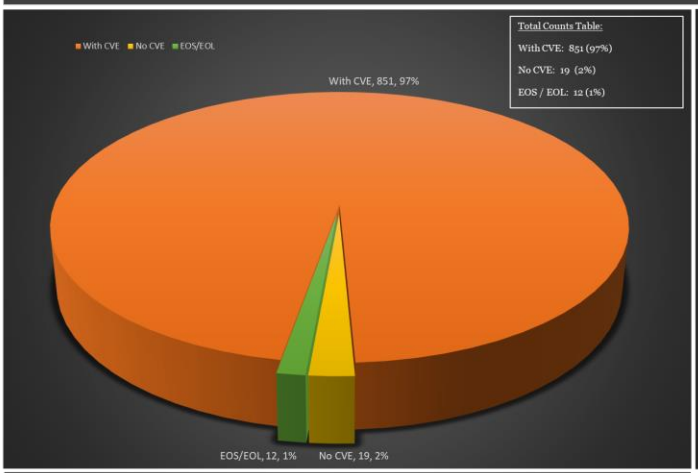
CLOUD SECURITY

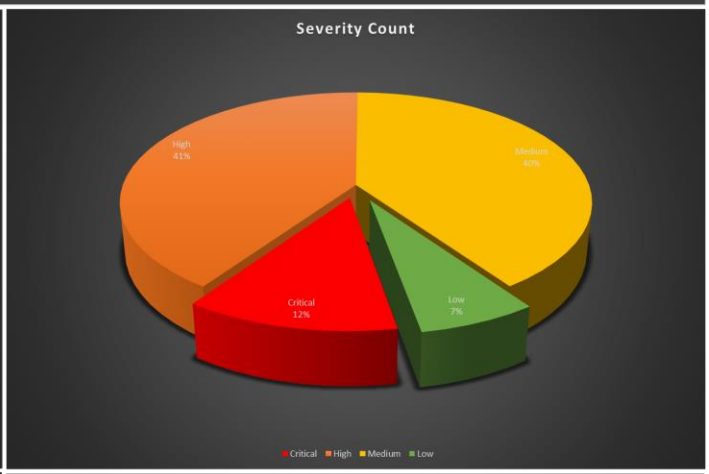
MANAGED DETECTION & RESPONSE

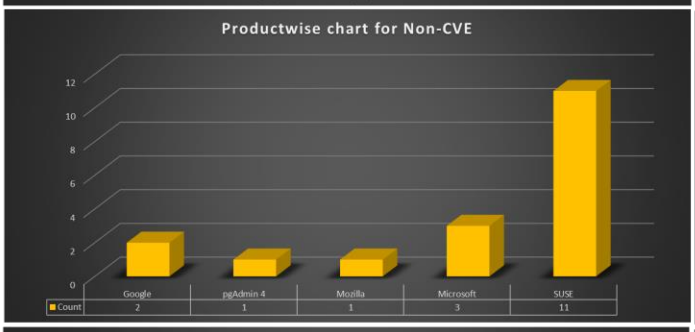
CHECK OUT OUR VULNERABILITY ADVISORY

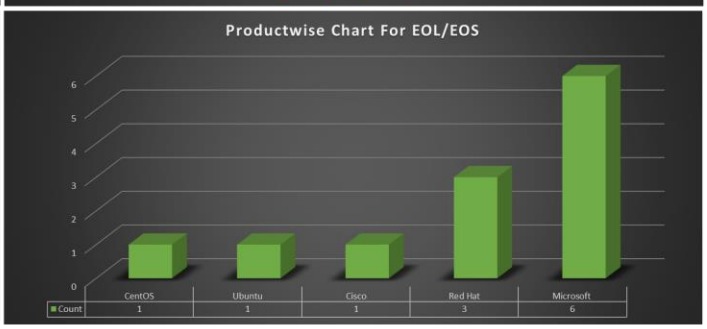
EXECUTIVE SUMMARY

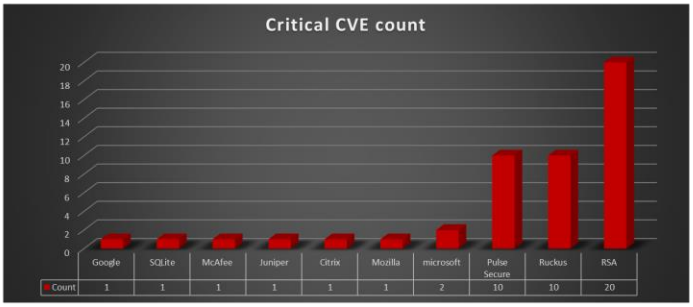


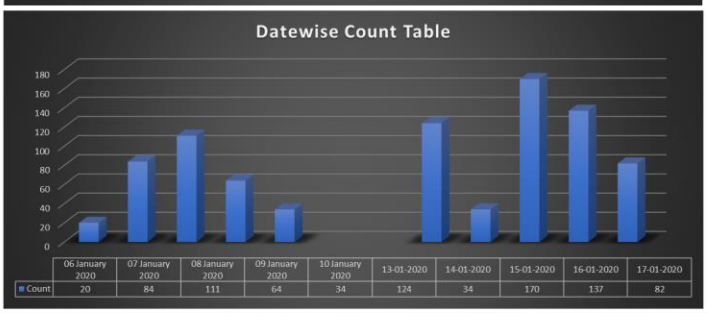


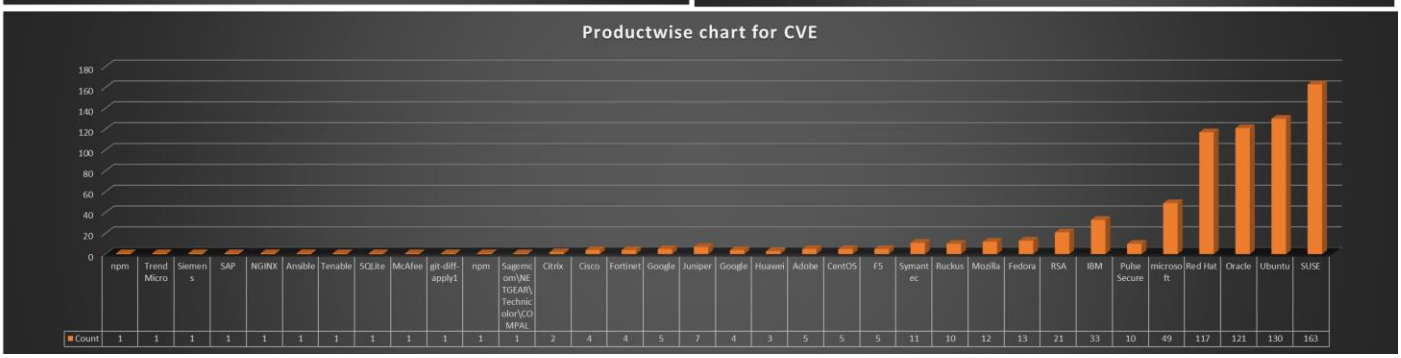












Top 10 Vulnerabilities of the week

Date	Sr. #	CVE ID	Vendor	Product	Summary	Recommendation
06-01-2020	1	CVE-2019-20218	SQLite	SQLite 3.30.1	A Critical Remote Unspecified Vulnerability was found in SQLite 3.30.1.	Updates are not available yet, users are requested to continuously monitor vendor site. https://www.sqlite.org/index.html
07-01-2020	2	CVE-2019-3663	McAfee	McAfee Advanced Threat Defense (ATD)	An Unprotected Storage of Credentials vulnerability in McAfee Advanced Threat Defense (ATD).	Advanced Threat Defense (ATD) Hotfix 4.6.2.18 contains the fix
07-01-2020	3	CVE-2019-17498, CVE-2019-10086, CVE-2019-10218, CVE-2019-3689, CVE-2019-15239, CVE-2019-15212, CVE-2019-15211, CVE-2019-15217, CVE-2019-15218, CVE-2019-15215, CVE-2018-20976, CVE-2019-15291, CVE-2019-15807, CVE-2019-15505, CVE-2019-15216, CVE-2019-15219, CVE-2019-15220, CVE-2019-15221, CVE-2019-16233, CVE-2019-10220	RSA	RSA Authentication Manager 8.4 patch P8 and earlier,	Multiple components within RSA Authentication Manager require a security update to address various vulnerabilities.	For RSA: The following RSA Authentication Manager releases contain resolutions to these vulnerabilities: RSA Authentication Manager 8.4 Patch 9 and later
08-01-2020	4	CVE-2019-17666	Google	Android	Google Android Code Execution Vulnerability in Kernel Components	Updates are available please see below updated reference link. Updated link: https://source.android.com/security/bulletin/pixel/2020-01-01 Updated link: https://source.android.com/security/bulletin/2020-01-01
08-01-2020	5	CVE-2019-19834, CVE-2019-19835, CVE- 2019-19836, CVE-2019-19837, CVE-2019-19838, CVE-2019-19839, CVE2019-19840, CVE-2019-19841, CVE-2019-19842, CVE-2019-19843	Ruckus	ZoneDirector and Unleashed product lines	A number of security vulnerabilities are found on the ZoneDirector and Unleashed product lines. Collectively, these vulnerabilities allow an attacker to perform the multiple actions.	Ruckus Networks is releasing the fix for these vulnerabilities through a software update. Because these are CRITICAL issues, all customers are strongly encouraged to apply the fix. Fixes are available in vendor link please see below Reference Link . https://www.ruckuswireless.com/security/299/view/pdf

08-01-2020	6	CVE-2019-17267	Juniper	Juniper Networks Contrail Networking	Multiple vulnerabilities in third party software used in Juniper Networks Contrail Networking have been resolved in release R1912..	These issues have been resolved in Contrail Networking release R1912.
13-01-2020	7	CVE-2019-19781	Citrix	Citrix Application Delivery Controller and Citrix Gateway	Vulnerability in Citrix Application Delivery Controller and Citrix Gateway leading to arbitrary code execution.	Updates are available please see below reference link. https://support.citrix.com/article/CTX267027
13-01-2020	8	CVE-2019-17026	Mozilla	Firefox 71 and Firefox ESR 68.3	ozilla developers reported memory safety bugs present in Firefox 71 and Firefox ESR 68.3 .	Fixed in: Firefox ESR 68.4 Fixed in: Firefox 72
14-01-2020	9	CVE-2019-11510, CVE-2019-11508, CVE-2019-11540, CVE-2019-11543, CVE-2019-11541, CVE-2019-11542, CVE-2019-11539, CVE-2019-11538, CVE-2019-11509, CVE-2019-11507	Pulse Secure	Pulse Secure VPN servers	Unpatched Pulse Secure VPN servers continue to be an attractive target for malicious actors.	The solution for these vulnerabilities is to upgrade your Pulse Connect Secure and Pulse Policy Secure server software version to the corresponding version that has the fix. Updates are available at Pulse Secure Advisory. https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101
14-01-2020	10	CVE-2020-0610, CVE-2020-0609	microsoft	Windows Server	A remote code execution vulnerability exists in Windows Remote Desktop Gateway (RD Gateway) when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests.	Updates are available. Please see the references or vendor advisory for more information. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0610 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0609