Sattrix

20th Jan – 31st 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

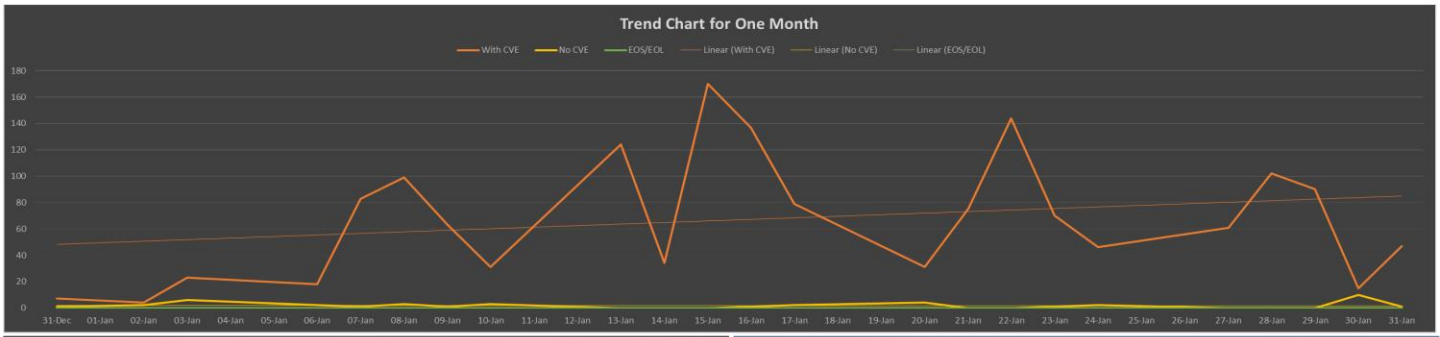
MANAGED SERVICES

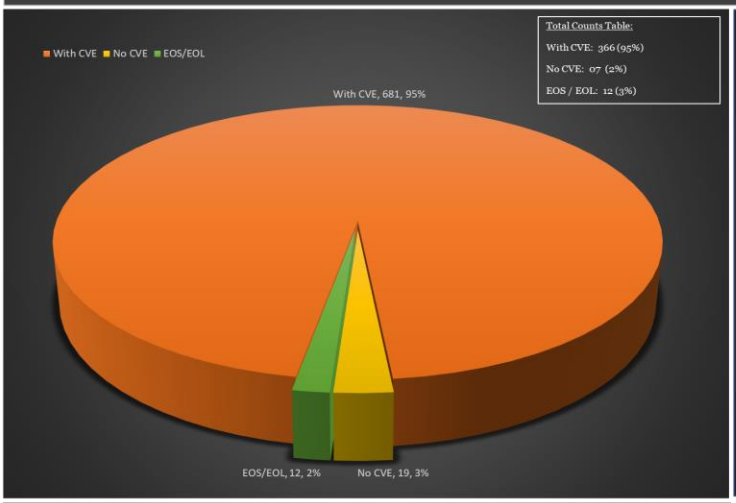
CLOUD SECURITY

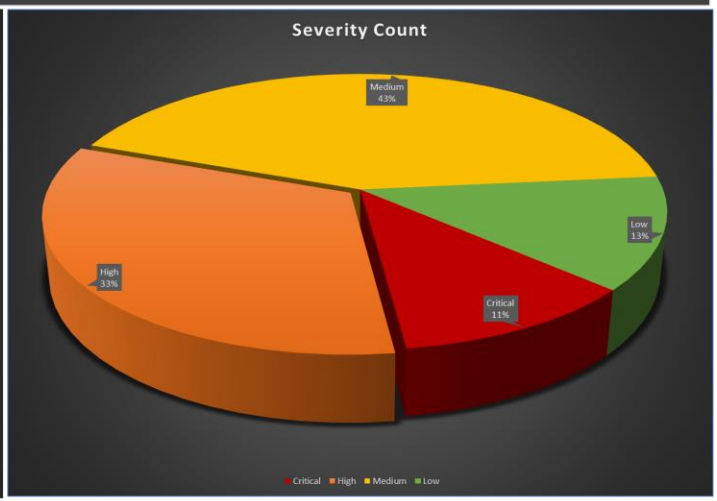
MANAGED DETECTION & RESPONSE

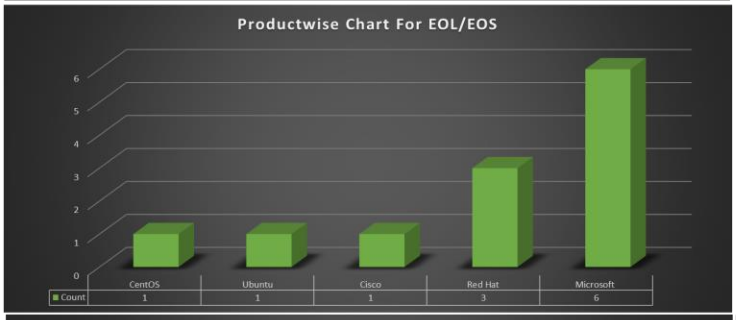
CHECK OUT OUR VULNERABILITY ADVISORY

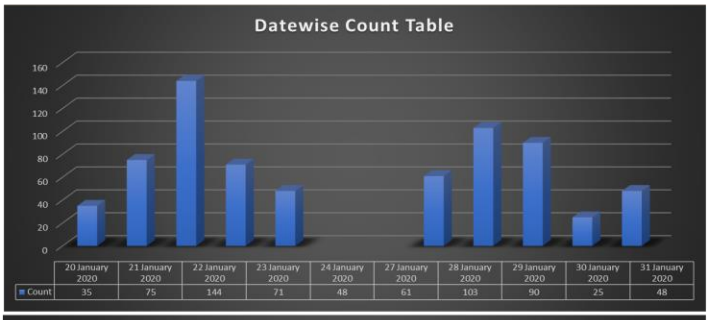
EXECUTIVE SUMMARY

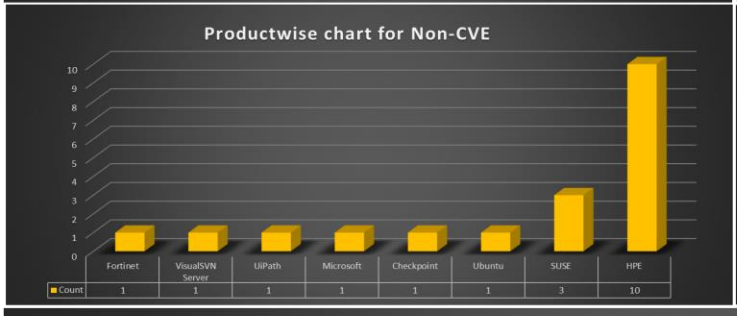


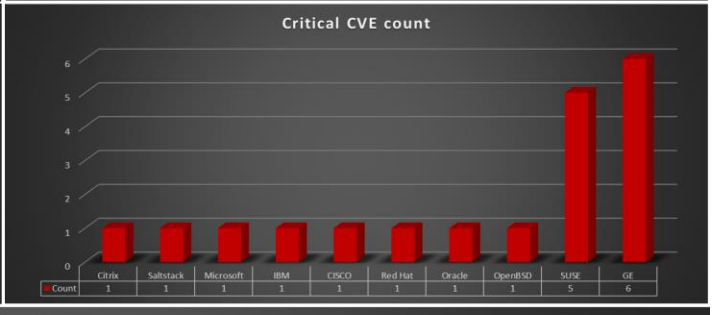


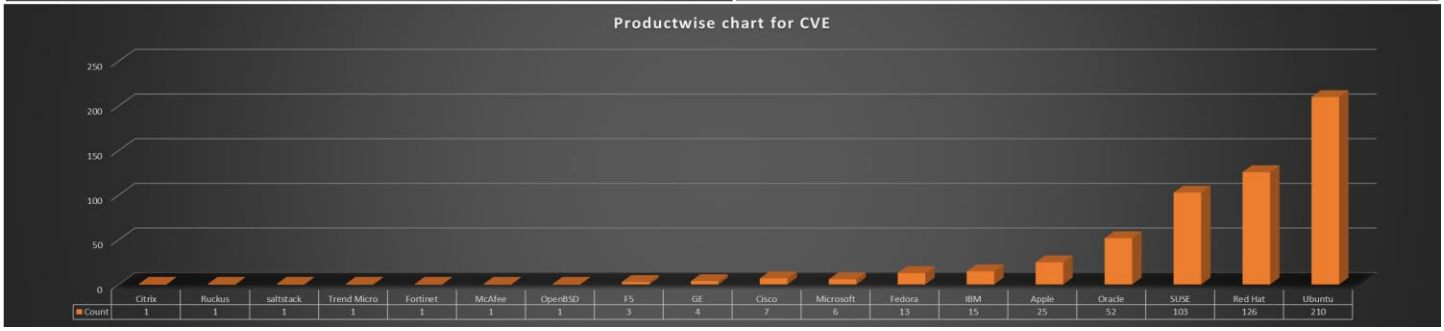












Top 10 Vulnerabilities of the week						
Date	**Sr. #**	**CVE ID**	**Vendor**	**Product**	**Summary**	**Recommendation**
20-01-2020	1	CVE-2019-19781	Citrix	Citrix Application Delivery Controller and Citrix Gateway	Vulnerability in Citrix Application Delivery Controller and Citrix Gateway leading to arbitrary code execution.	Updates are available please see below reference link. https://support.citrix.com/article/CTX267027
20-01-2020	2	CVE-2019-17361	Saltstack	Salt Before version 2019.2.0	This allows an unauthenticated attacker with network access to the API endpoint to execute arbitrary code on the salt-api host.	It is recommended to upgrade to version 2019.2.3 or a later one.
20-01-2020	3	CVE-2020-0674	Microsoft	Internet Explorer 9,10,11	An attacker who successfully exploited the vulnerability could gain the same user rights as the current user.	Updates are available. Please see the references or vendor advisory for more information. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200001
20-01-2020	4	CVE-2019-11043	IBM	IBM API Connect - V5.0.0.0-5.0.8.7, IBM API Connect - V2018.4.1.0-2018.4.1.8	IBM API Connect has addressed the following vulnerability	Updates are available please see below reference link https://www.ibm.com/support/pages/node/1172398
21-01-2020	5	CVE-2019-2126, CVE-2019-9232, CVE-2019-9325, CVE-2019-9371, CVE-2019-9433	SUSE	SUSE Linux Enterprise Server 15-LTSS	An update that fixes 5 vulnerabilities is now available.	Updates are available please see below reference link. https://www.suse.com/support/update/announcement/2020/suse-su-20200143-1/
23-01-2020	6	CVE-2019-16028	CISCO	Cisco Firepower Management Center-6.2.3,6.3.0,6.4.0,6.5.0,6.6.0	A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an unauthenticated, remote attacker to bypass authentication and execute arbitrary actions with administrative privileges on an affected device.	Fixed For - 6.5.0.1, 6.4.0.7 Updates are available please see below reference link. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20200122-fmc-auth https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvr95287
23-01-2020	7	CVE-2019-5544	Red Hat	Red Hat Enterprise Linux 6	An update for openslp is now available for Red Hat Enterprise Linux 6.	Updates are available please see below reference link. https://access.redhat.com/security/cve/cve-2019-5544

24-01-2020	8	CVE-2020-6962, CVE-2020-6961, CVE-2020-6963, CVE-2020-6964, CVE-2020-6965, CVE-2020-6966	GE	ApexPro Telemetry Server, Versions 4.2 and prior, CARESCAPE Telemetry Server, Versions 4.2 and prior, Clinical Information Center (CIC), Versions 4.X and 5.X, CARESCAPE Central Station (CSCS), Versions 1.X	Successful exploitation of these vulnerabilities could occur when an attacker gains access to the mission critical (MC) and/or information exchange (IX) networks due to improper configuration or physical access to devices.	Updates are available please see below reference link. https://www.us-cert.gov/ics/advisories/icsma-20-023-01
27-01-2020	9	CVE-2020-2555	Oracle	Oracle Coherence (12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0), Oracle Coherence - 3.7.1.17	Successful attacks of this vulnerability can result in takeover of Oracle Coherence.	Patches are available please see below reference link. Updated link: https://www.oracle.com/security-alerts/cpujan2020.html
30-01-2020	10	CVE-2020-7247	OpenBSD	OpenSMTPD (6.4.0, 6.4.0p1, 6.4.0p2, 6.4.1, 6.4.1p1, 6.4.1p2, 6.4.2, 6.4.2p1, 6.6.0, 6.6.0p1, 6.6.1, 6.6.1p1)	Successful exploitation of this vulnerability may result in complete compromise of vulnerable system.	Install updates from vendor\'s website. https://www.cybersecurity-help.cz/vdb/openbsd/https://seclists.org/oss-sec/2020/q1/40