SECURITY INTELLIGENCE ADVISORY

31st AUG - 11th SEP 2020

OUR LOCATIONS

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

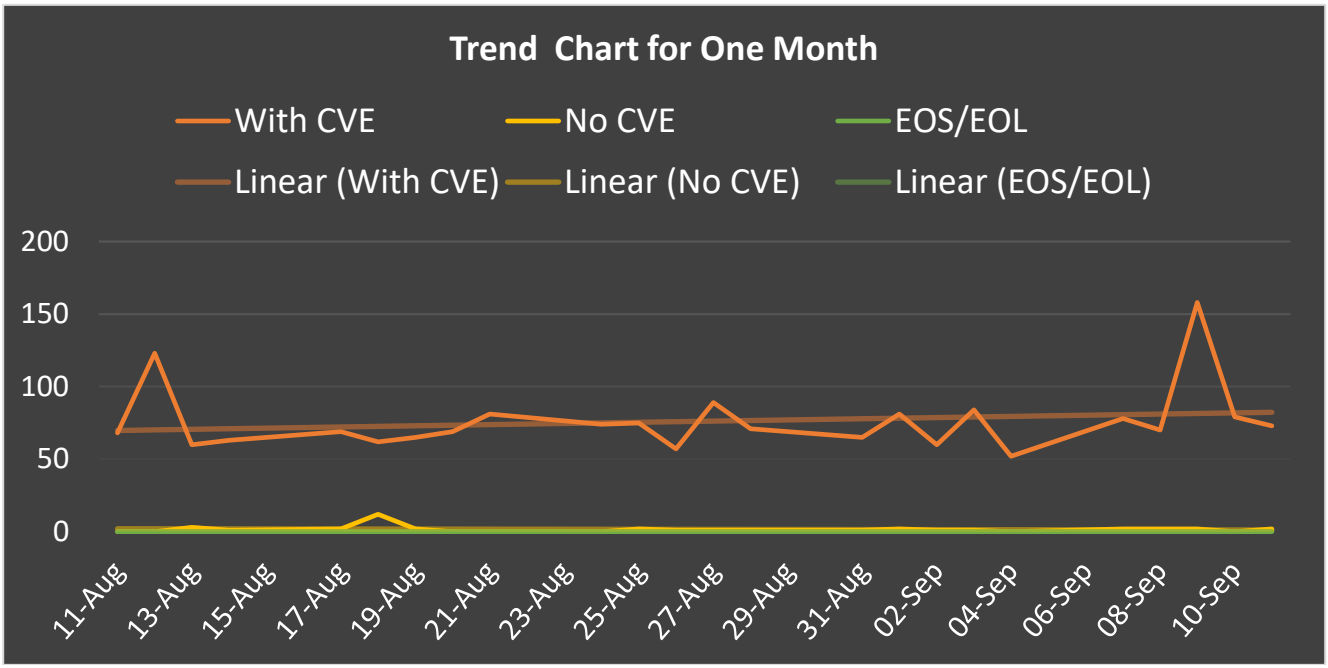
Every organization – large, medium and small has a huge risk and a typical challenge of managing vulnerabilities present in the operating systems, Vulnerabilities that are not attended possess a very high risk and can cost your organization various threats and damage. There is threat from users within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

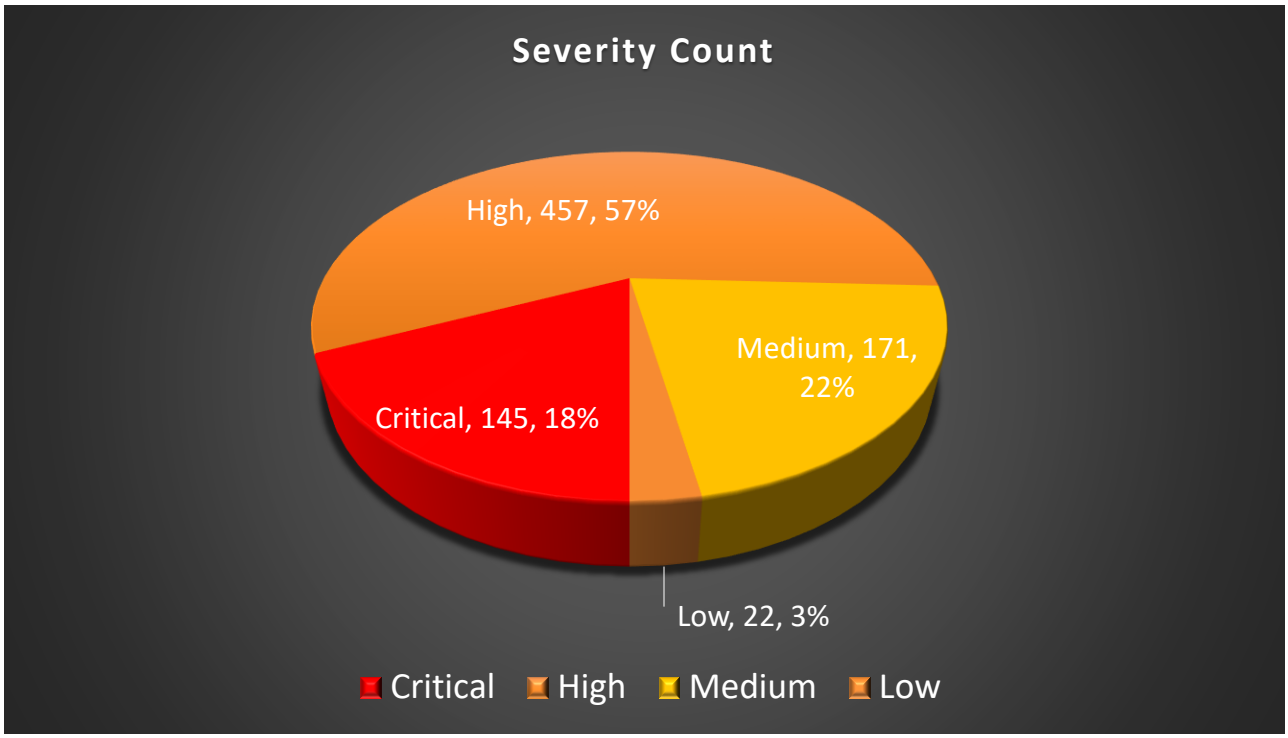
1. We monitor around 2000 applications, appliances and operating systems, and tests and verifies the vulnerabilities reported in them.
2. We are focusing each vulnerability disclosed in those 2000 products.
3. The systems and applications monitored by Sattrix Research Team are those in use in the environment of the customers.
4. 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.
5. The Vulnerability Database covers vulnerabilities that can be exploited in all types of products – software, hardware, firmware, etc.
6. 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.
7. The Vulnerability Database covers vulnerabilities that can be exploited in all types of products and also, we cover zero days and EOS/EOL.
8. 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.
9. The Sattrix Advisory descriptions include severity, under investigation product, Affected Product, cve id, Sattrix score, reference links and remediations.
10. Sattrix researchers monitor the vulnerabilities within 5 business working days.

EXECUTIVE SUMMARY

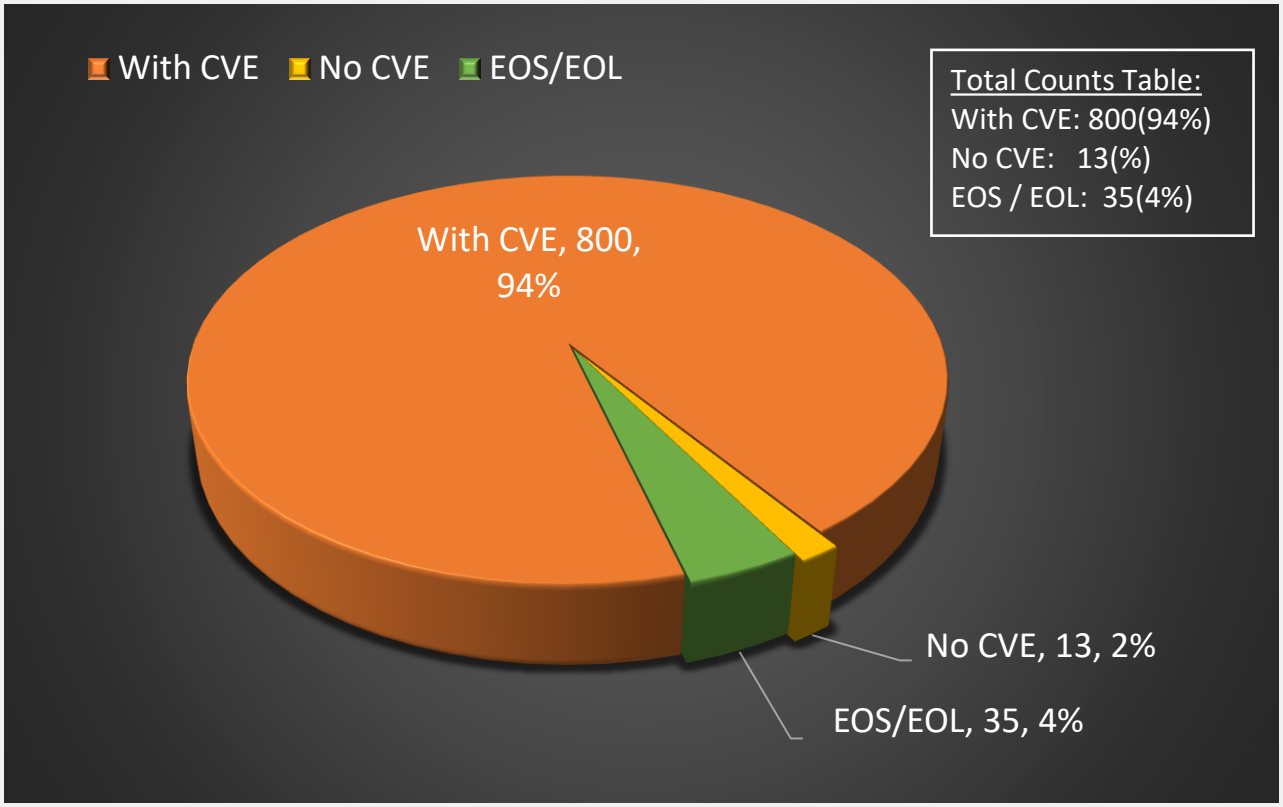
- Overall Monthly Vulnerability Trend Chart



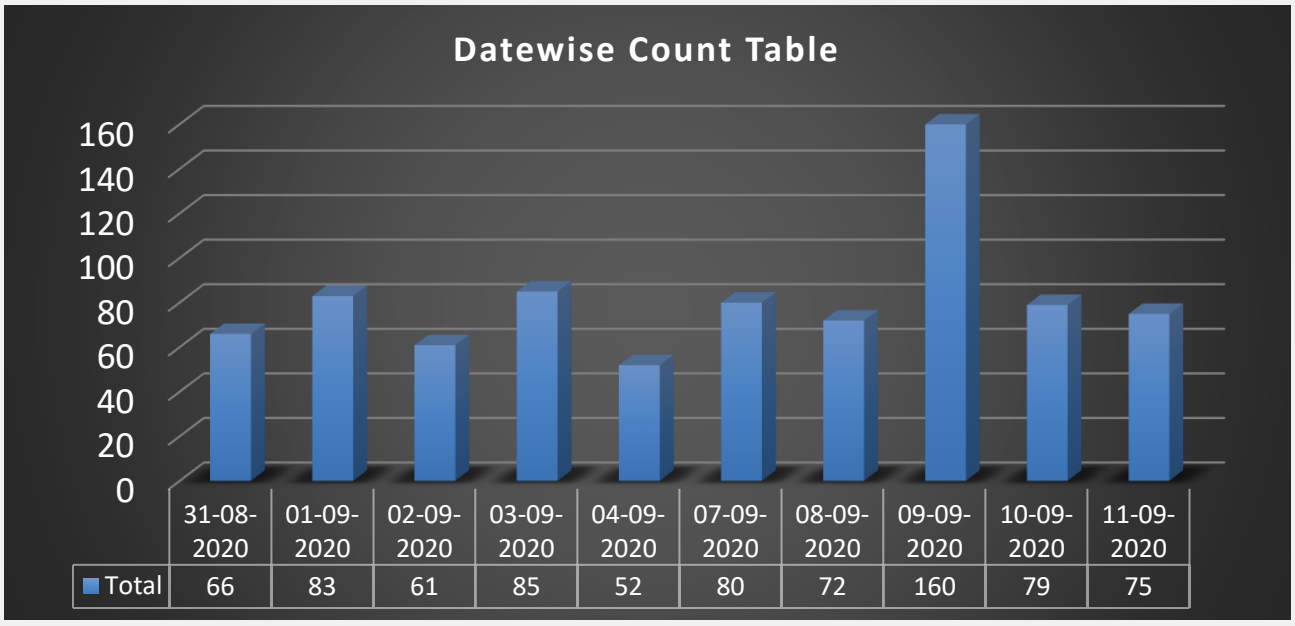
- Released Vulnerabilities and severity wise count
  - This graph present threat levels based on vulnerability identified.



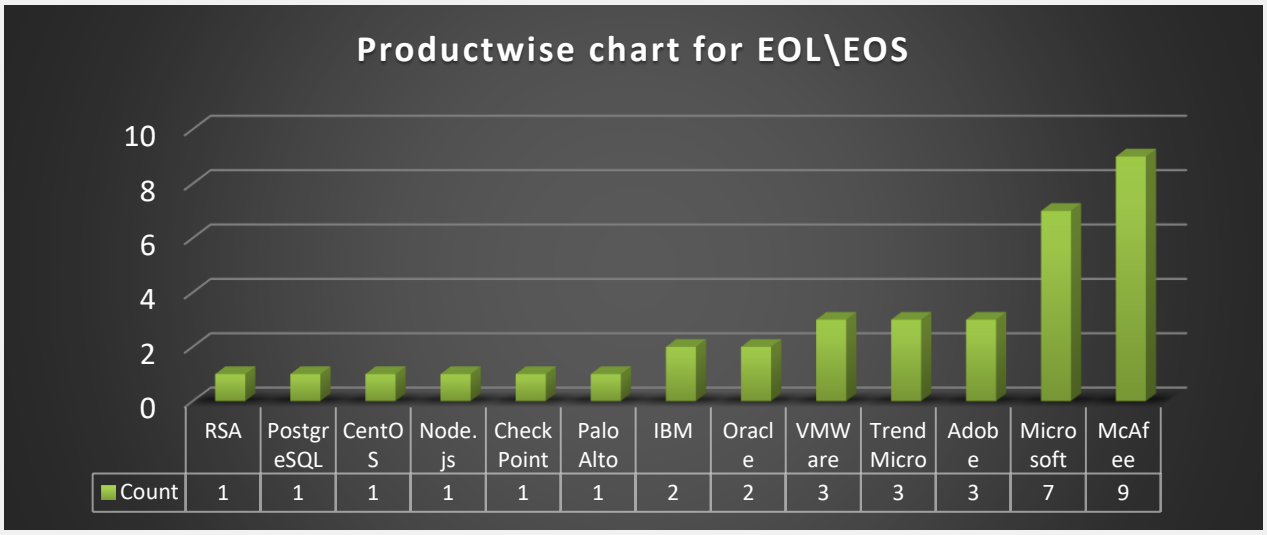
- This graph present total released vulnerabilities including Zero-day vulnerability and EOS/EOL with their count.



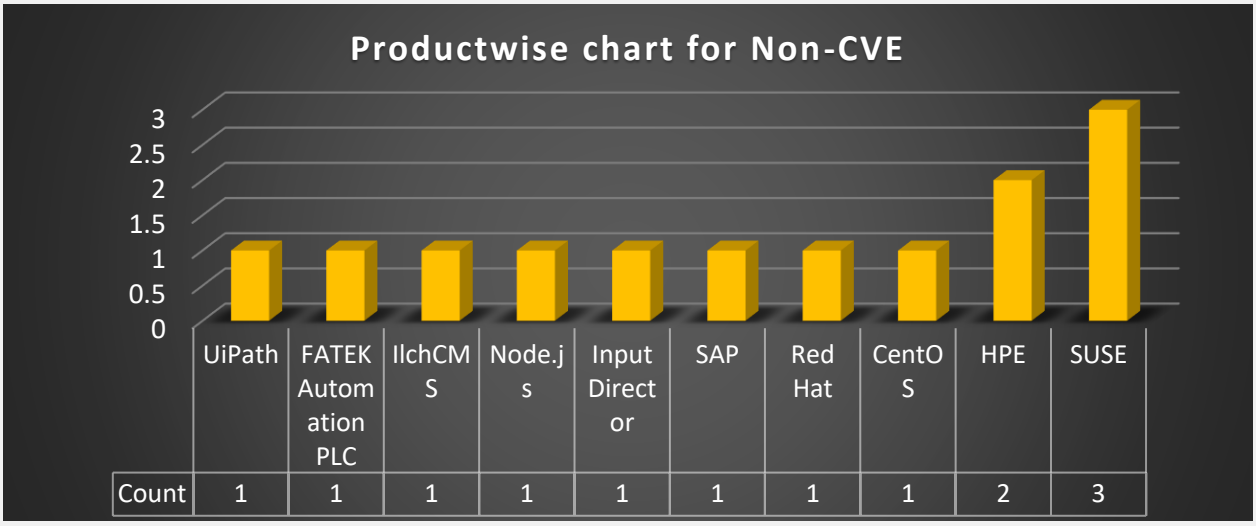
- Date wise Released Vulnerabilities Count, fortnightly summarized



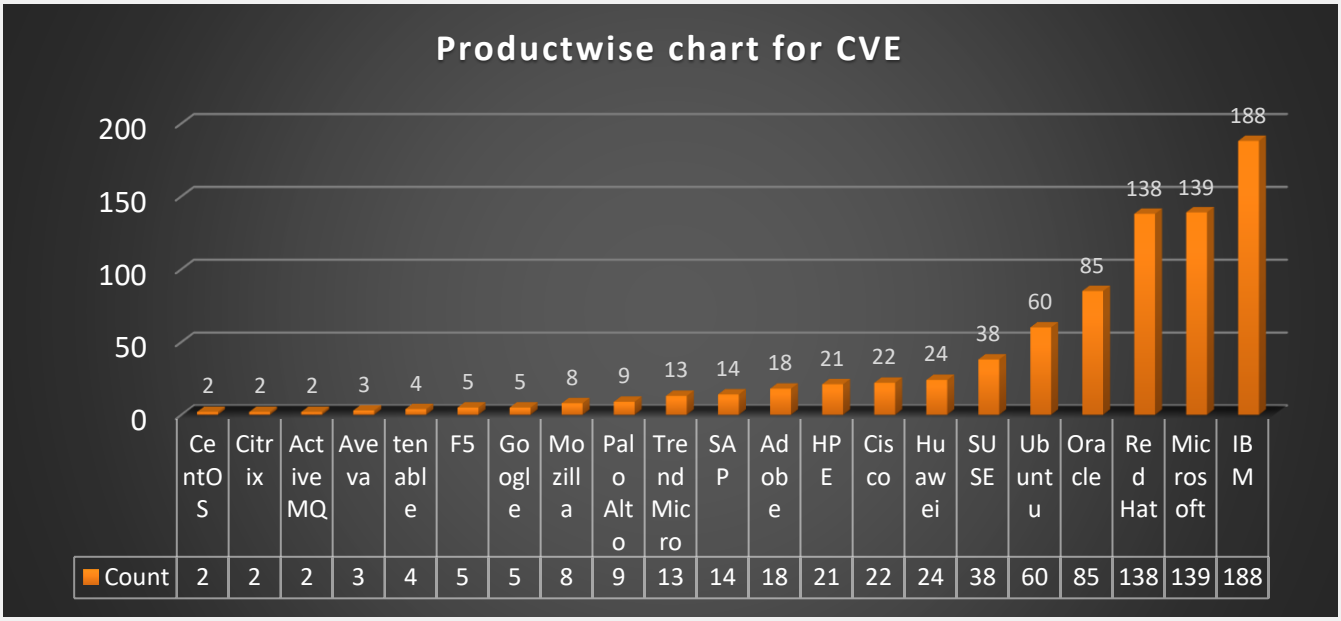
- Product wise Released EOS/EOL count.



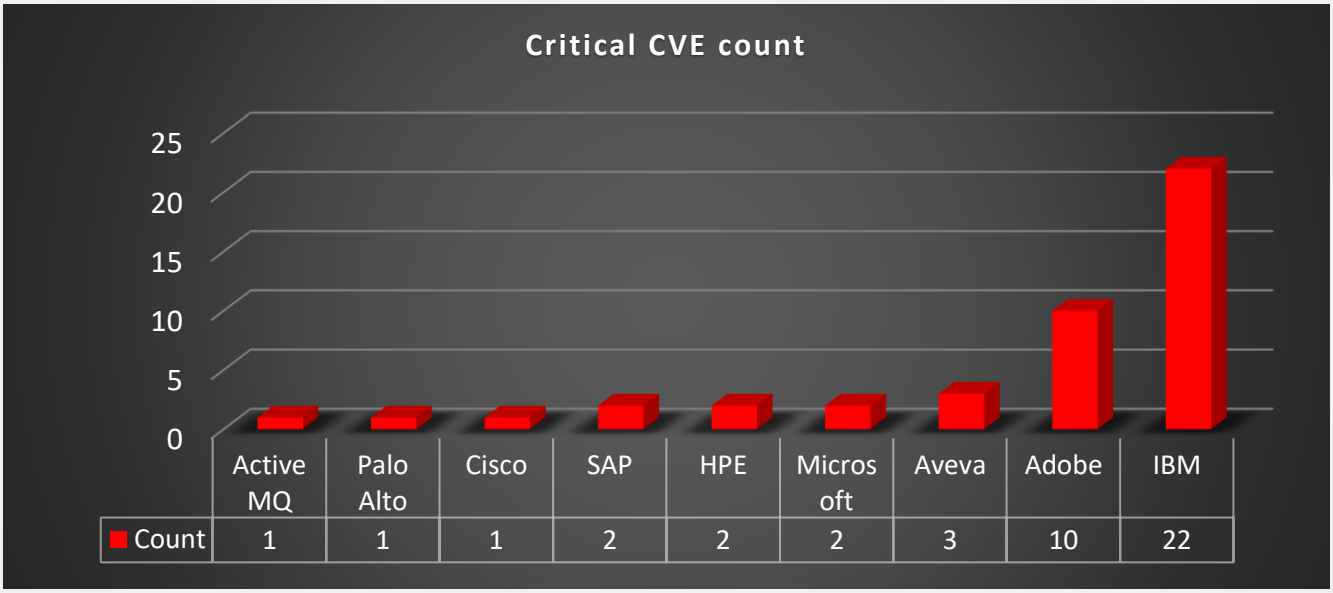
- Product wise Released Non-CVE ID or Zero Day vulnerabilities count.



- Product wise Released vulnerabilities count.



- Top 10 Vulnerabilities product wise critical vulnerabilities



Top Vulnerabilities of the Week						
Date	**Sr. #**	**CVE ID**	**Vendor**	**Product**	**Summary**	**Recommendation**
31-08-2020	1	CVE-2018-8014, CVE-2020-1938	HPE	HP-UX Tomcat-based Servlet v.7.x Engine D.7.0.84.01 and earlier	Local: Access Restriction Bypass; Remote: Access Restriction Bypass, Code Execution, Denial of Service (DoS), Gain Unauthorized Access, URL Redirection, Unauthorized Access to Data, Unauthorized Access to Sensitive Information	Updates are available please see below reference link. https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbux04015en_us
01-09-2020	2	CVE-2017-15095, CVE-2017-17485, CVE-2018-11307, CVE-2018-12022, CVE-2018-12023, CVE-2018-14718, CVE-2018-14719, CVE-2018-14720, CVE-2018-14721, CVE-2018-19360, CVE-2018-19361, CVE-2018-19362, CVE-2018-5968, CVE-2018-7489, CVE-2019-12086, CVE-2019-12384, CVE-2019-12814, CVE-2019-14379, CVE-2019-14439, CVE-2019-14540, CVE-2019-14892, CVE-2020-9548	IBM	IBM Security Guardium Insights - 2.0.1	IBM Security Guardium Insights is affected by Components with known vulnerabilities	Updates are available please see below reference link https://www.ibm.com/support/pages/node/6324739

02-09-2020	3	CVE-2020-3495	Cisco	Cisco Jabber for Windows - 12.8(2)	A vulnerability in Cisco Jabber for Windows could allow an authenticated, remote attacker to execute arbitrary code.	Updates are available please see below reference link https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-jabber-UyTKCPGg
09-09-2020	4	CVE-2020-1182 CVE-2020-16857	Microsoft	Dynamics 365 for Finance and Operations	Microsoft Dynamics 365 for Finance and Operations (on-premises) Remote Code Execution Vulnerability	Updates are available please see below reference link. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1182 https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16857
09-09-2020	5	CVE-2020-9727 CVE-2020-9728 CVE-2020-9729 CVE-2020-9730 CVE-2020-9731	Adobe	Adobe InDesign - 15.1.1 and below	Adobe has released a security update for Adobe InDesign.	Updates are available please see below reference link. https://helpx.adobe.com/security/products/indesign/apsb20-52.html
09-09-2020	6	CVE-2020-9732, CVE-2020-9734, CVE-2020-9740, CVE-2020-9741, CVE-2020-9742	Adobe	Adobe Experience Manager (AEM) - 6.5.6.0, 6.4.8.2 , AEM Forms add-on - AEM Forms Service Pack 6	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/experience-manager/apsb20-56.html
09-09-2020	7	CVE-2020-6286, CVE-2020-6287	SAP	SAP NetWeaver AS JAVA (LM Configuration Wizard); Versions - 7.30, 7.31, 7.40, 7.50	Multiple Vulnerabilities in SAP NetWeaver AS JAVA (LM Configuration Wizard)	Updates are available please see below reference link. https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=552599675

10-09-2020	8	CVE-2020-2040	Palo Alto	All versions of PAN-OS 8.0, PAN-OS 8.1 versions earlier than PAN-OS 8.1.15, PAN-OS 9.0 versions earlier than PAN-OS 9.0.9, PAN-OS 9.1 versions earlier than PAN-OS 9.1.3	Palo Alto Networks PAN-OS is vulnerable to a stack-based buffer overflow, caused by improper bounds checking by the PAN-OS management web interface. By sending a specially crafted request to the Captive Portal or Multi-Factor Authentication interface, a remote authenticated attacker could overflow a buffer to execute arbitrary code on the system with root privileges.	Refer to Palo Alto Networks Security Advisories for patch, upgrade or suggested workaround information. See References. https://security.paloaltonetworks.com/CVE-2020-2040
11-09-2020	9	CVE-2020-11998	ActiveMQ	Apache ActiveMQ 5.15.12	Apache ActiveMQ could allow a remote attacker to execute arbitrary code on the system, caused by improper input validation by the RMIConnectorServer function.	Updates are available please see below reference link https://exchange.xforce.ibmcloud.com/vulnerabilities/188065 http://activemq.apache.org/
11-09-2020	10	CVE-2020-1351, CVE-2020-13499, CVE-2020-13500	Aveva	AVEVA Enterprise Data Management Web	AVEVA Enterprise Data Management Web is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database.	Updates are available please see below reference link https://exchange.xforce.ibmcloud.com/vulnerabilities/188129 https://exchange.xforce.ibmcloud.com/vulnerabilities/188128 https://exchange.xforce.ibmcloud.com/vulnerabilities/188125https://www.aveva.com/en/products/enterprise-data-management/