Red Piranha
unified threat management

Threat Intelligence Report

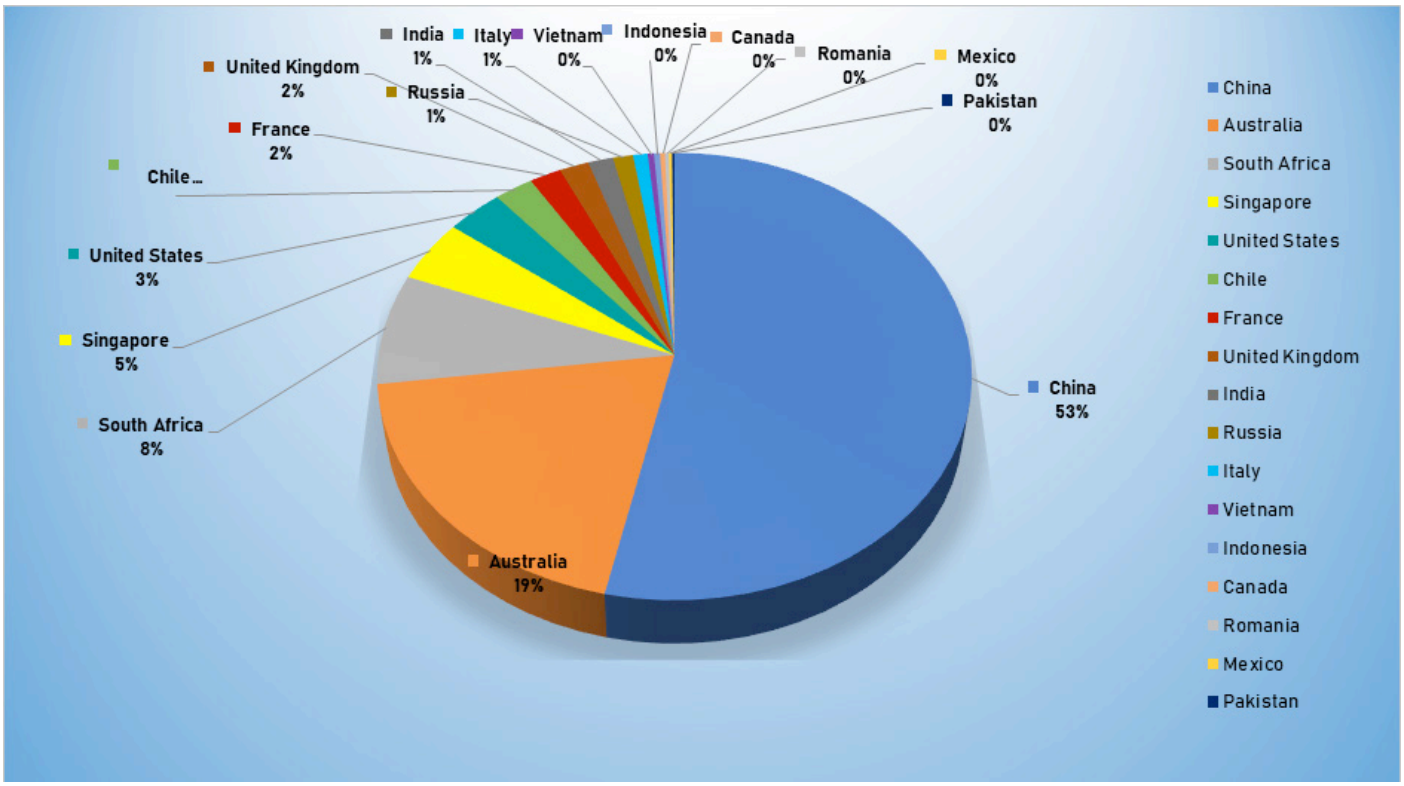
November 25 - December 1, 2019

Trends

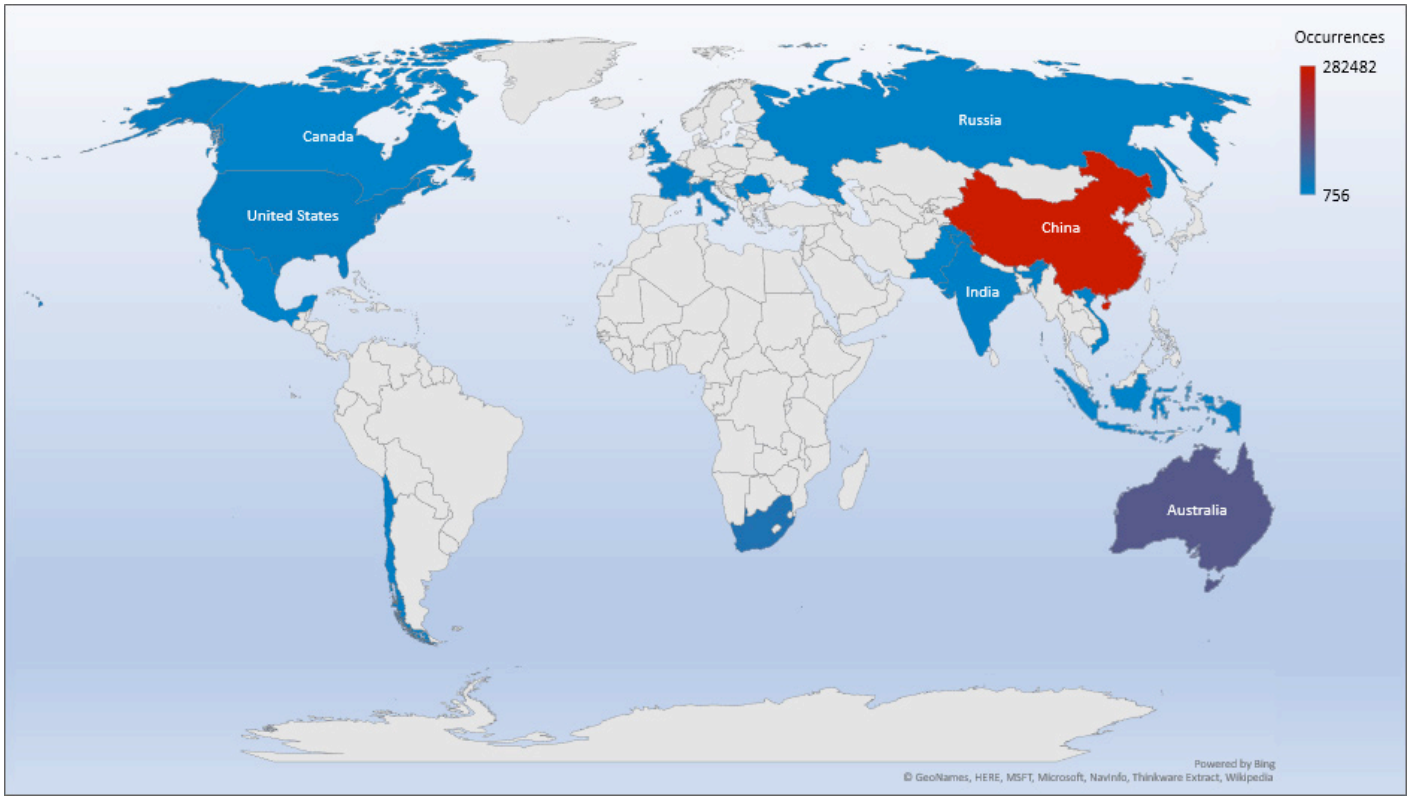
- **The top attacker country was China with 282482 unique attackers (53%).**
- **The top Exploit event was Authentication with 32% of occurrences.**
- **The top Trojan C&C server detected was Heodo with 50 instances detected.**

Top Attacker by Country

Country	Occurrences	Percentage
China	282482	53.36%
Australia	103018	19.46%
South Africa	42345	8.00%
Singapore	23964	4.53%
United States	17922	3.39%
Chile	12375	2.34%
France	9952	1.88%
United Kingdom	9355	1.77%
India	7886	1.49%
Russia	6358	1.20%
Italy	4566	0.86%
Vietnam	1968	0.37%
Indonesia	1905	0.36%
Canada	1549	0.29%
Romania	1224	0.23%
Mexico	992	0.19%
Pakistan	785	0.15%
Serbia	756	0.14%
Argentina	583	0.11%

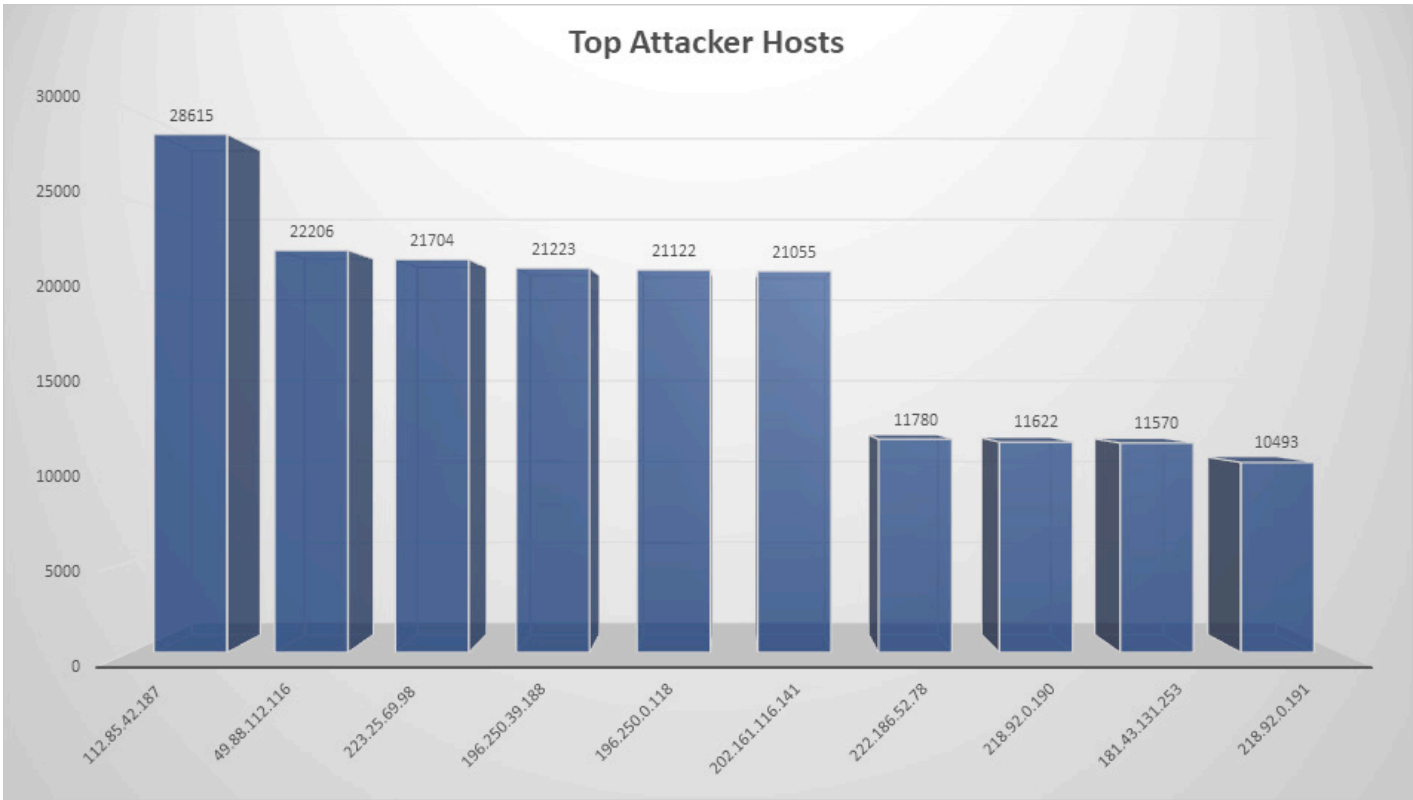


Threat Geo-location



Top Attacking Hosts

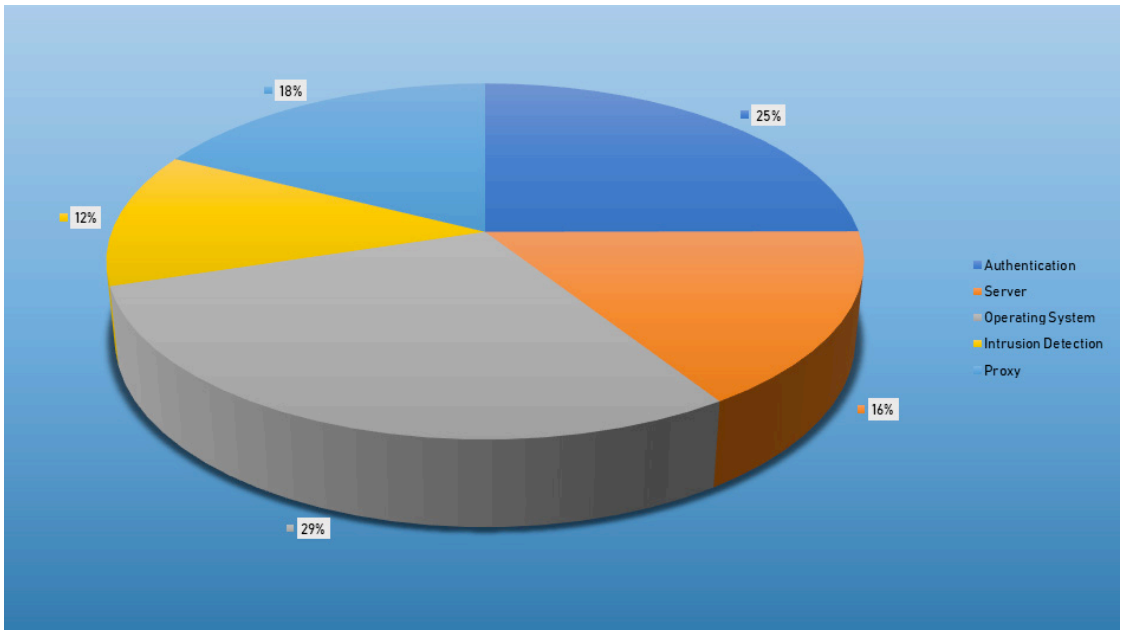
Host	Occurrences
112.85.42.187	28615
49.88.112.116	22206
223.25.69.98	21704
196.250.0.118	21122
202.161.116.141	21055
222.186.52.78	11780
218.92.0.190	11622
181.43.131.253	11570
218.92.0.191	10493

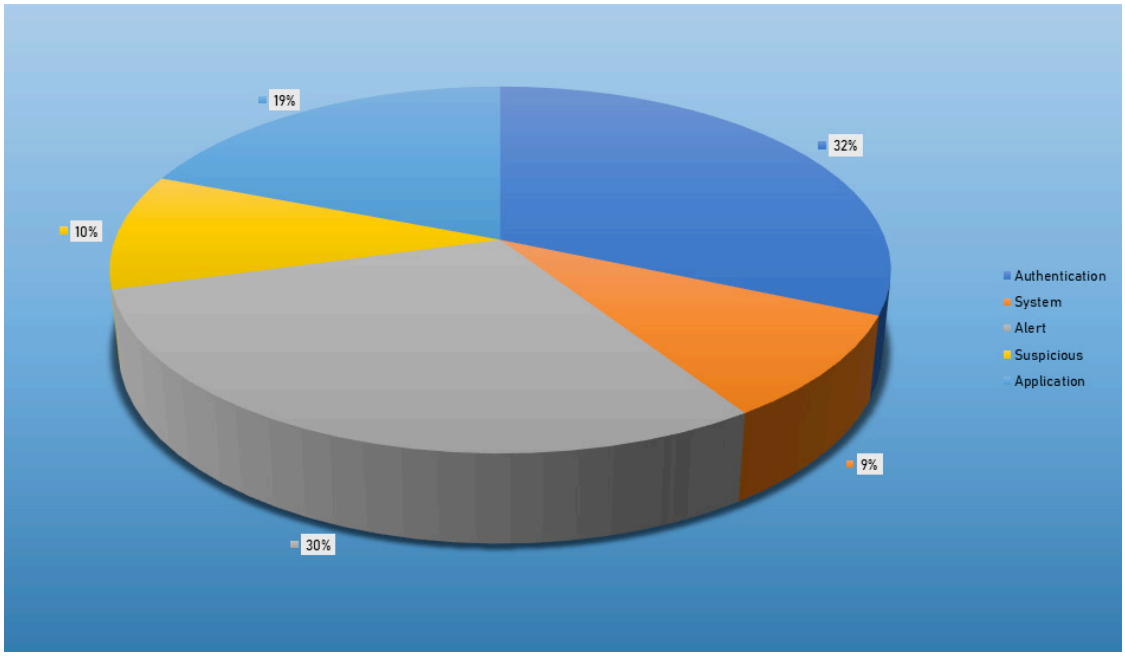


Top Network Attackers

Origin AS	Country	Description
4837	China	CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
4134	China	CHINANET-BACKBONE No.31,Jin-rong Street, CN
56300	Singapore	MYREPUBLIC-SG MyRepublic Ltd., SG
37515	South Africa	iCONNECT, ZA
7545	Australia	TPG-INTERNET-AP TPG Telecom Limited, AU
23650	China	CHINANET-JS-AS-AP AS Number for CHINANET jiangsu province backbone, CN

Top Event NIDS and Exploits

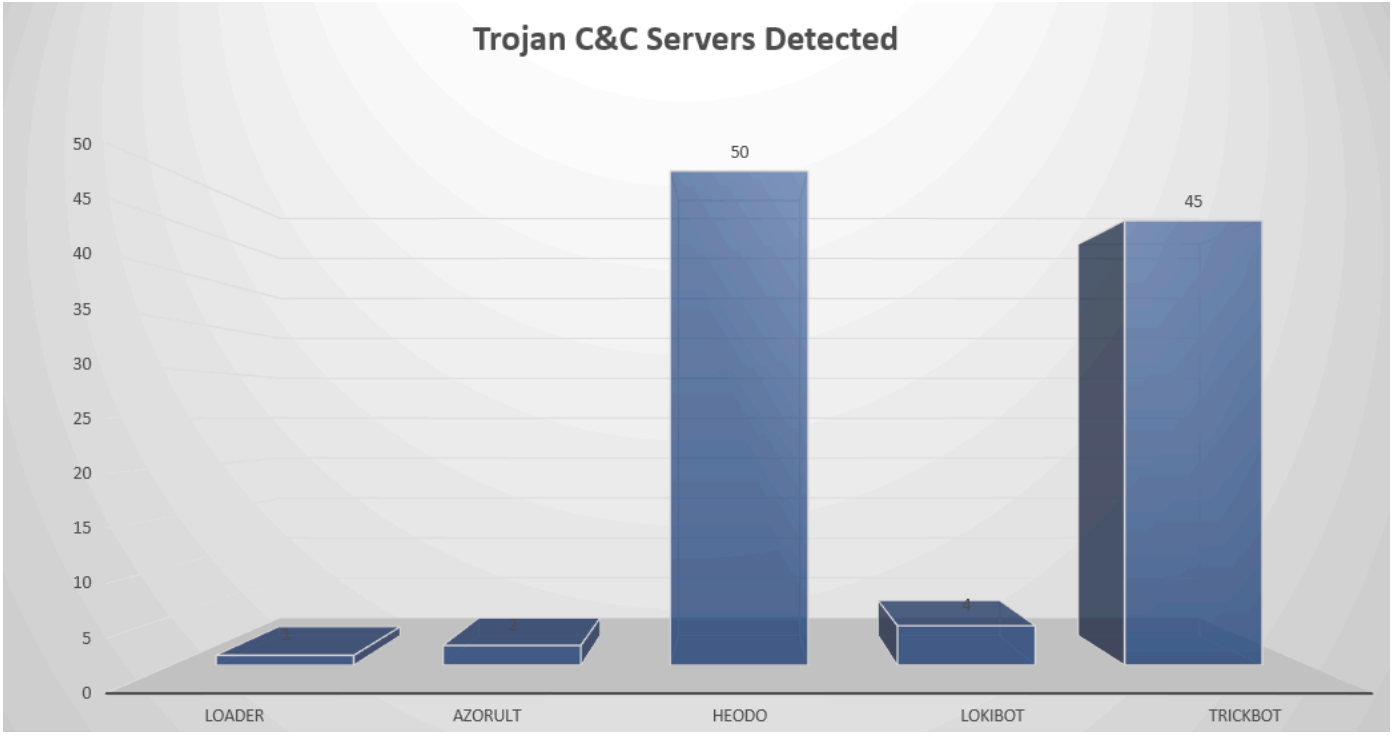




Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
Loader	1	185.204.2.218
AZORult	2	83.166.251.55, 185.222.57.75
Heodo	50	107.2.2.28, 116.48.138.115, 118.200.218.193, 189.180.105.125, 122.11.164.183, 172.90.70.168, 200.71.193.220, 47.50.251.130, 197.90.159.42, 109.166.89.91, 211.218.105.101, 190.12.119.180, 120.150.246.241, 197.254.221.174, 195.244.215.206, 190.186.164.23, 47.187.70.124, 2.38.99.79, 125.230.36.147, 72.27.212.209, 85.105.183.228, 187.250.92.82, 41.218.118.66, 95.219.199.225, 81.213.145.45, 77.211.249.124, 187.190.49.92, 12.229.155.122, 5.88.182.250, 128.65.154.183, 201.183.251.100, 195.226.144.249, 186.0.68.43, 190.17.42.79, 54.38.94.197, 45.56.88.91, 59.110.18.236, 80.211.32.88, 50.63.13.135, 51.68.220.244, 185.234.72.64, 24.45.193.161, 142.127.57.63, 186.66.224.182, 203.130.0.69, 80.93.48.49, 192.161.190.171, 104.236.137.72, 206.189.112.148, 206.81.10.215
Lokibot	4	216.10.240.90, 107.175.150.73, 80.249.144.204, 185.159.153.129

Name	Number Discovered	Location
TrickBot	45	212.73.150.4, 188.165.62.47, 146.185.253.175, 94.156.35.206, 162.244.32.52, 162.247.155.113, 167.86.123.83, 51.89.73.144, 103.75.117.188, 45.141.100.190, 107.181.187.221, 85.217.170.153, 5.2.77.78, 192.227.173.100, 5.2.72.102, 82.118.21.57, 5.182.210.30, 66.55.71.151, 85.204.116.154, 172.245.159.121, 194.5.250.121, 192.227.232.46, 198.15.119.79, 172.82.152.140, 81.177.22.39, 85.143.221.75, 37.46.135.95, 45.132.19.197, 185.99.2.115, 146.185.219.50, 146.185.253.174, 66.85.173.56, 185.174.173.143, 195.123.221.232, 51.89.73.148, 5.2.76.197, 45.138.157.23, 188.225.10.47, 81.177.181.222, 185.90.61.107, 46.17.105.97, 188.120.251.251, 2.57.184.9, 51.254.69.222, 5.34.176.212



Common Malware

MD5	Filename	Claimed Product	Detection Name
c5608e40f6f47ad84e2985804957c342	FlashHelperServices.exe	FlashHelper Service	PUA:2144 Flash Player-tpd
ef048c07855b3ef98bd991c413bc73b1	xme64-501.exe	N/A	PUA.Win.Dropper.Razy::tpd
e2ea315d9a83e7577053f52c974f6a5a	c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f.bin	N/A	W32.Agent WDCR: Gen.21 gn.1201
b77c0c1ed4cff895bf862cf46b601c84	opCS.gif	N/A	W32.C29DA492E7-100.SBX.TG
718d579ea6ea48f95225cc9c794f9703	opext.gif	N/A	W32.4DAC88A67B-100.SBX.TG

CVEs For Which Public Exploits Have Been Detected

CVE, Title, Vendor	Description	CVSS v2 Base Score	Date Created	Date Updated
CVE-2019-1429 Microsoft Windows Scripting Engine Memory Corruption Vulnerability **Microsoft**	An information disclosure vulnerability exists when Microsoft Edge based on Edge HTML improperly handles objects in memory. An attacker who successfully exploited the vulnerability could obtain information to further compromise the users system. To exploit the vulnerability, in a web-based attack scenario, an attacker could host a website in an attempt to exploit the vulnerability.	7.6	11/12/19	11/12/19
CVE-2019-18862 GNU Mailutils Privilege Escalation Vulnerability **GNU**	The --url parameter included in the GNU Mailutils maidag utility can be used to write to arbitrary files on the host operating system. By default, maidag is set to execute with setuid root permissions, which can lead to local privilege escalation through code/command execution by writing to the system's crontab or by writing to other root owned files on the operating system.		11/11/19	11/11/19
CVE-2018-14665 Xorg X11 Server Local Privilege Escalation Vulnerability **Multi-Vendor**	A flaw was found in xorg-x11-server where an incorrect permission check for -modulepath and -logfile options are set when starting Xorg. X server allows unprivileged users with the ability to log in to the system via physical console to escalate their privileges and run arbitrary code under root privileges.	7.2	10/25/18	10/22/19
CVE-2019-11539 Pulse Secure VPN Arbitrary Command Execution Vulnerability **Pulse Secure**	Pulse Secure VPN with admin web interface allows an authenticated attacker to inject and execute commands. An attacker can exploit these issues to access arbitrary files in the context of the application, write arbitrary files, hijack an arbitrary session and gain unauthorized access, execute arbitrary script code in the browser of an unsuspecting user in the context of the affected site, obtain sensitive information, inject and execute arbitrary commands and execute arbitrary code in the context of the application.	6.5	04/25/19	08/09/19

CVE, Title, Vendor	Description	CVSS v2 Base Score	Date Created	Date Updated
CVE-2019-16113 Bludit Directory Traversal Image File Upload Vulnerability **Bludit**	Bludit allows remote code execution via bl kernel/ajax/ upload-images.php because PHP code can be entered with a .jpg file name, and then this PHP code can write other PHP code to a ../ pathname.	6.5	09/08/19	11/12/19
CVE-2019-11409 FusionPBX Operator Panel exec.php Command Execution Vulnerability **FusionPBX**	app/ operator_panel/ exec.php in the Operator Panel module in FusionPBX suffers from a command injection vulnerability due to a lack of input validation that allows authenticated non-administrative attackers to execute commands on the host. This can further lead to remote code execution when combined with an XSS vulnerability also present in the FusionPBX Operator Panel module.	6.5	06/17/19	06/18/19
CVE-2019-17671 WordPress Unauth'ed view Posts Vulnerability **WordPress**	Wordpress versions allows unauthenticated view of private/draft posts. Unauthenticated viewing of certain content is possible because the static query property is mishandled. This vulnerability could allow an unauthenticated user to view private or draft posts due to an issue within WP_Query.	5.0	10/17/19	11/05/19