Red Piranha
unified threat management

Threat Intelligence Report

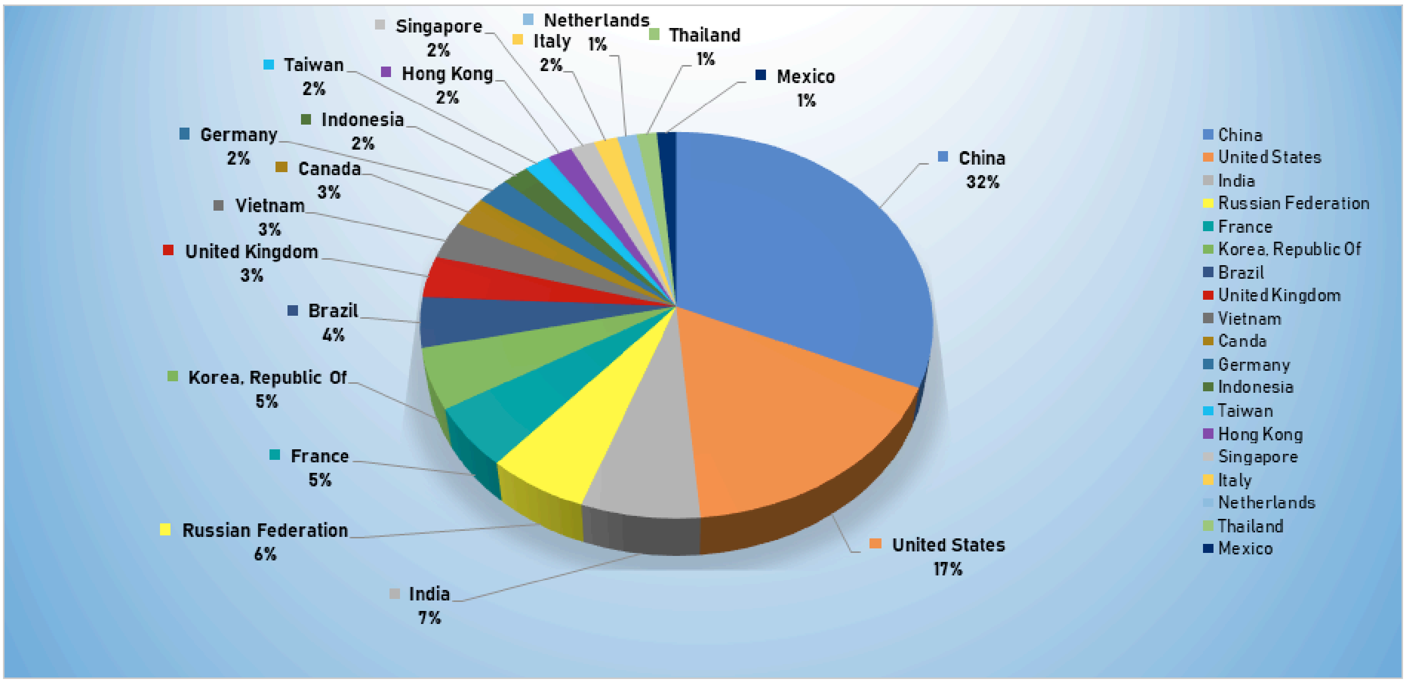
October 21-27 2019

Trends

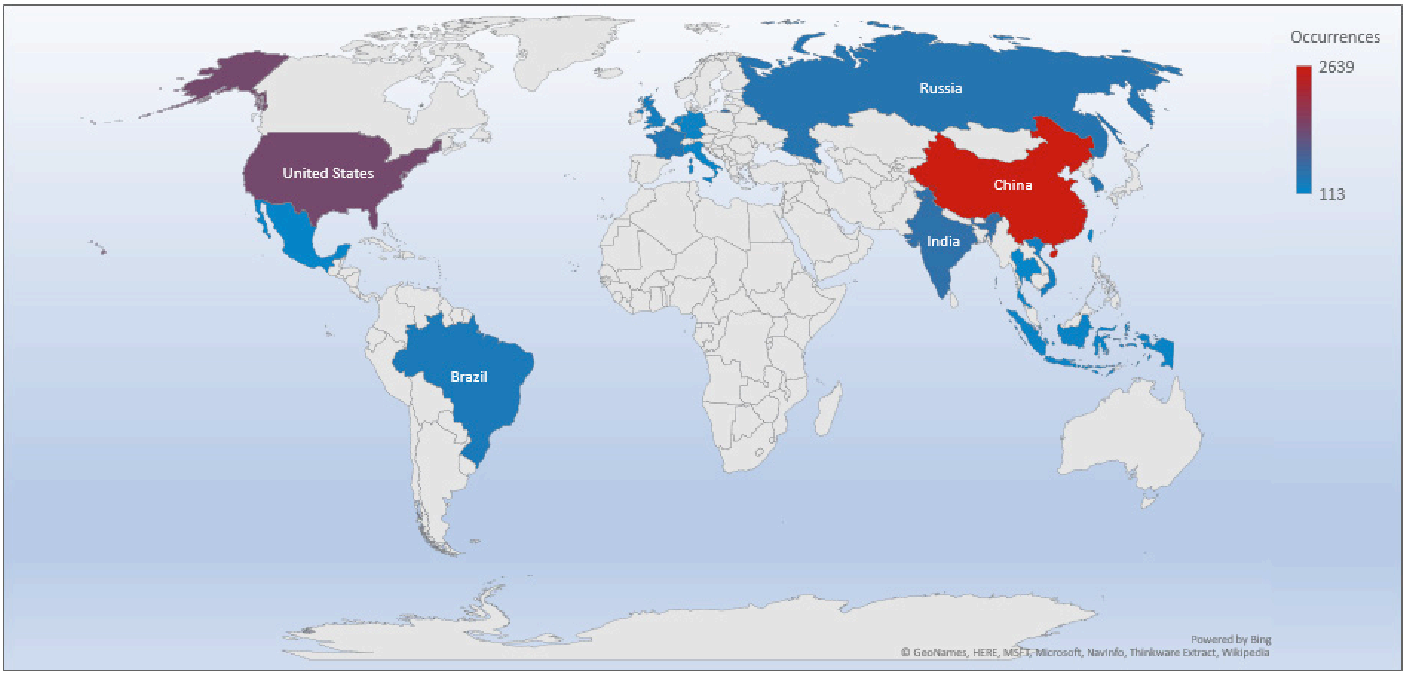
- **The top attacker country was China with 2639 unique attackers (32%).**
- **The top Exploit event was Authentication with 54% of occurrences.**
- **The top Trojan C&C server detected was Trickbot with 65 instances detected.**
- **The most prevalent malware detected was Bitcoin Miner xme64-2141.exe, first seen 10th March 2019.**

Top Attacker by Country

Country	Occurrences	Percentage
China	2639	31.71%
United States	1409	16.93%
India	571	6.86%
Russian Federation	483	5.80%
France	431	5.18%
Korea	424	5.09%
Brazil	353	4.24%
United Kingdom	289	3.47%
Vietnam	262	3.15%
Canada	213	2.56%
Germany	190	2.28%
Indonesia	151	1.81%
Taiwan	149	1.79%
Hong Kong	142	1.71%
Singapore	139	1.67%
Italy	135	1.62%
Netherlands	115	1.38%
Thailand	114	1.37%
Mexico	113	1.36%

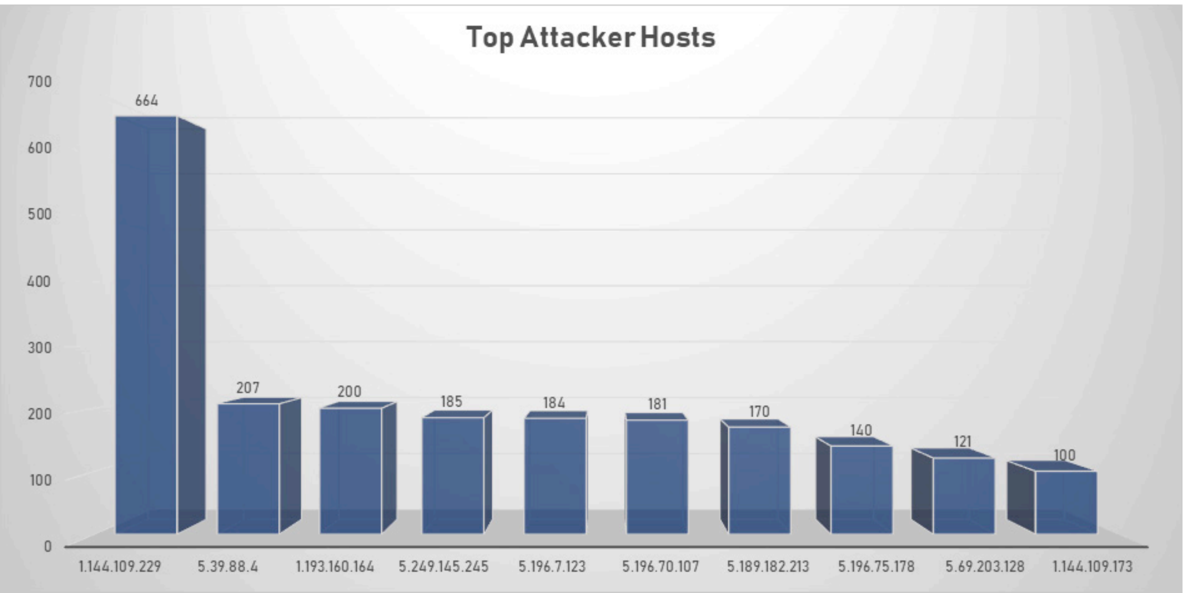


Threat Geo-location


Occurrences
2639
113
Russia
China
India
United States
Brazil
Powered by Bing
© GeoNames, HERE, MSFT, Microsoft, Navinfo, Thinkware Extract, Wikipedia

Top Attacking Hosts

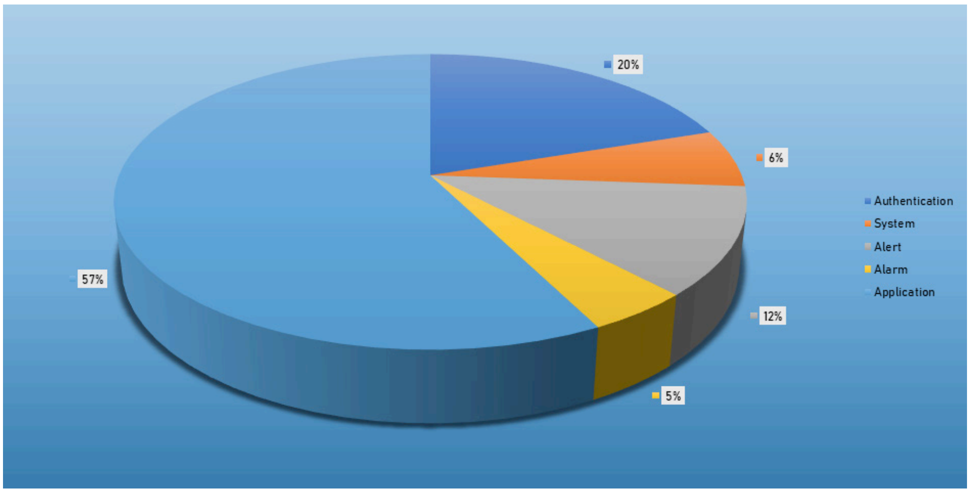
Host	Occurrences
1.144.109.229	664
5.39.88.4	207
1.193.160.164	200
5.249.145.245	185
5.196.7.123	184
5.196.70.107	181
5.189.182.213	170
5.196.75.178	140
5.69.203.128	121
1.144.109.173	100
112.85.42.187	28
218.92.0.191	7

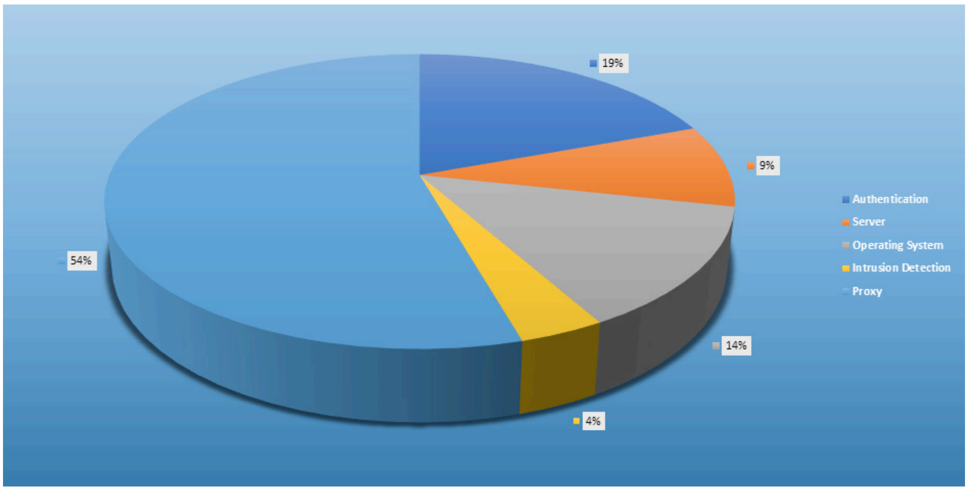


Top Network Attackers

Origin AS	Announcement	Description
AS1221	1.128.0.0/11	Telstra
AS16276	5.39.0.0/17	OVH SAS
AS4134	1.192.0.0/13	CHINANET henan province network
AS31034	5.249.144.0/21	Aruba S.p.A. - Cloud Services Farm2

Top Event NIDS and Exploits



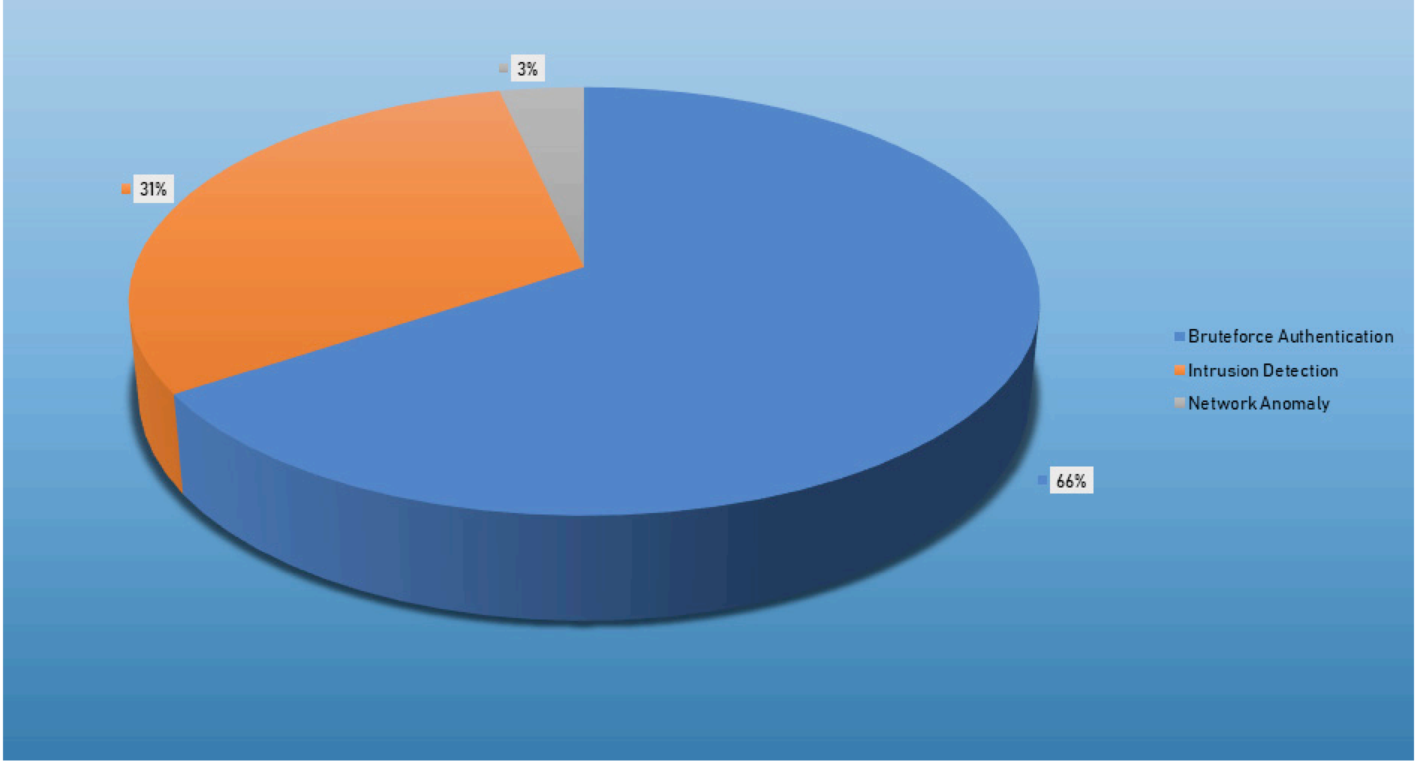


Top Alarms

Type of Alarm	Occurrences
Bruteforce Authentication	1772
Intrusion Detection	834
Network Discovery	95

Comparison from last week

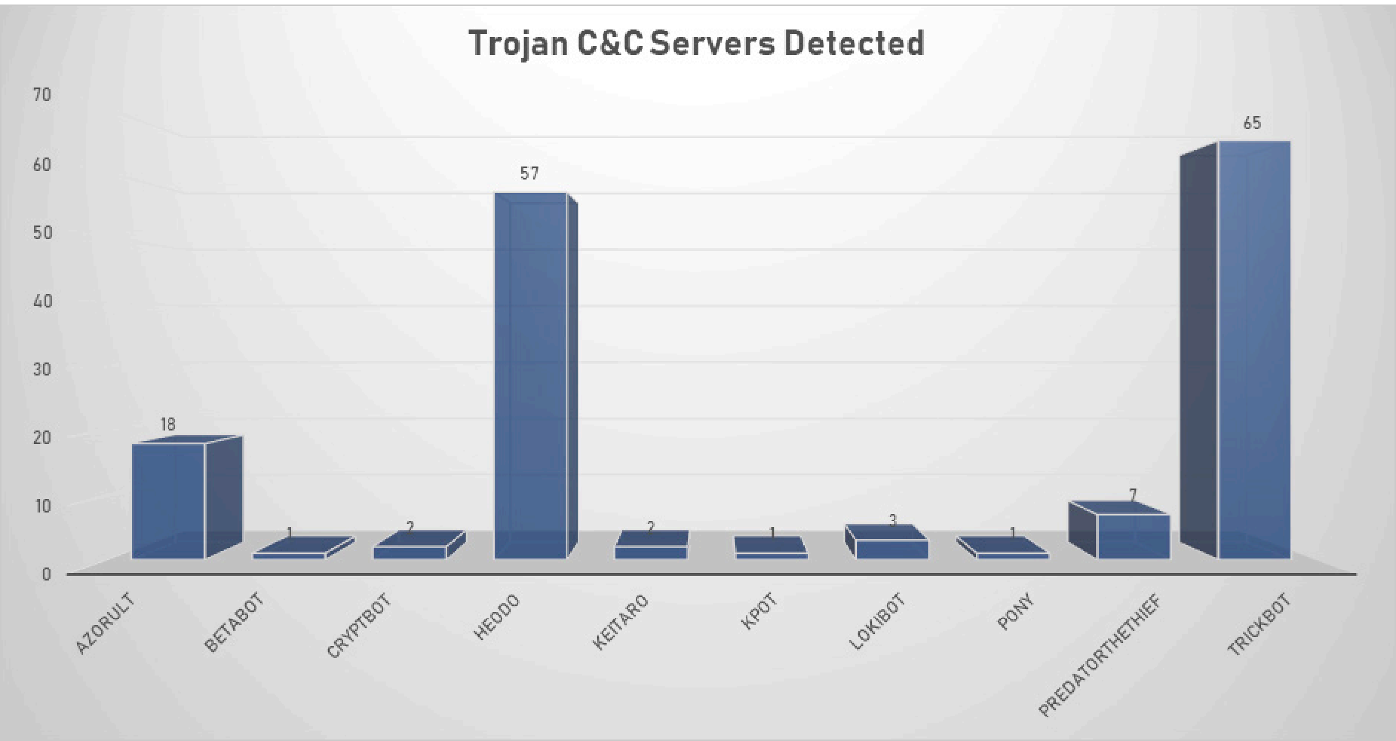
Type of Alarm	Occurrences
DatabaseAttack - Stored Procedure Access —Attack	81
Bruteforce Authentication	43
Network Anomaly	2



Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
Azorult	18	167.86.123.249, 185.212.130.104, 185.212.130.17, 185.212.130.34, 185.212.130.39, 185.212.130.50, 185.212.130.54, 185.212.130.56, 185.212.130.69, 185.212.130.70, 185.212.130.74, 185.212.130.78, 185.212.130.8, 185.212.130.87, 194.67.90.231, 45.86.180.5, 93.189.43.82, babillonngloball.xyz
Betabot	1	111.90.142.117
CryptBot	2	185.151.245.99 , 195.133.144.68
Heodo	57	133.167.80.63, 144.139.158.155, 144.76.62.10, 148.72.151.34, 173.249.157.58, 173.249.47.77, 179.12.170.88, 181.16.17.210, 181.197.2.80, 181.230.126.152, 181.29.164.248, 181.47.235.26, 184.82.233.15, 185.45.24.254, 186.109.91.136, 186.23.132.93, 186.92.11.143, 187.155.233.46, 187.193.89.61, 189.159.113.125, 189.166.13.109, 189.218.243.150

Name	Number Discovered	Location
Heodo		189.253.27.123, 190.113.146.128, 190.120.104.21, 190.166.25.99, 190.217.1.149, 190.228.212.165, 198.199.114.69, 198.199.88.162, 200.30.227.135, 200.90.86.170, 201.106.32.171, 201.184.105.242, 201.213.32.59, 201.250.11.236, 201.250.54.115, 203.99.188.11, 203.99.188.203, 213.138.100.98, 216.98.148.181, 23.229.115.217, 23.239.29.211, 24.45.195.162, 37.187.2.199, 45.33.54.74, 45.56.122.75, 68.183.190.199, 70.32.94.58, 79.127.57.43, 85.25.255.207, 85.25.92.96, 86.98.25.30, 91.109.5.28, 91.204.163.19, 91.83.93.105, 96.20.84.254
Keitaro	2	5.188.231.211, 5.8.88.124
Kpot	1	111.90.142.117
LokiBot	3	194.67.206.57, 47.254.66.50, 91.211.245.184
Pony	1	137.59.54.74
PredatorTheThief	7	129.226.56.28, 193.124.186.171, 5.188.60.6, 5.8.88.64, 91.243.80.13, 92.63.197.238, 45.128.184.2



Common Malware

Malware Type	MD5	Typical Filename
W32.7ACF71AFA8-95.SBX.TG	4a50780ddb3db16ebab57b0ca42da0fb	xme64-2141.exe
W32.46B241E3D3-95.SBX.TG	db69eaaea4d49703f161c81e6fdd036f	xme32-2141-gcc.exe
W32.AgentWDCR:Gen.21gn.1201	e2ea315d9a83e7577053f52c974f6a5a	c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f.bin
W32.WNCryLdrA:Trojan.22k2.1201	8c80dd97c37525927c1e549cb59bcbf3	Eternalblue-2.2.0.exe
W32.Generic:Gen.22fz.1201	799b30f47060ca05d80ece53866e01cc	mf2016341595.exe

CVEs For Which Public Exploits Have Been Detected

ID: CVE-2019-14287
Title: SUDO Security Policy Bypass Vulnerability
Vendor: Multi-Vendor

Description: When sudo is configured to allow a user to run commands as an arbitrary user via the ALL keyword in a Runas specification, it is possible to run commands as root by specifying the user ID -1 or 4294967295. This can be used by a user with sufficient sudo privileges to run commands as root even if the Runas specification explicitly disallows root access as long as the ALL keyword is listed first in the Runas specification. An attacker with access to a Runas ALL sudoer account can bypass certain policy blacklists and session PAM modules, and can cause incorrect logging, by invoking sudo with a crafted user ID.

CVSS v2 Base Score: 7.2 (AV:L/AC:L/Au:N/C:C/I:C/A:C)

ID: CVE-2019-2215
Title: Android Binder Use-After-Free Vulnerability
Vendor: Google
Description: A use after free in binder.c allows an elevation of privilege from an application to the Linux Kernel. No user interaction is required to exploit this vulnerability, however exploitation does require either the installation of a malicious local application or a separate vulnerability in a network facing application.
CVSS v2 Base Score: 4.6 (AV:L/AC:L/Au:N/C:P/I:P/A:P)

ID: CVE-2019-7609
Title: Kibana Timelion Remote Code Execution Vulnerability
Vendor: Elastic
Description: Kibana Timelion visualizer is exposed to an arbitrary code execution vulnerability. An attacker with access to the Timelion application could send a request that will attempt to execute javascript code. This could possibly lead to an attacker executing arbitrary commands with permissions of the Kibana process on the host system.
CVSS v2 Base Score: 10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

ID: CVE-2019-16278
Title: Nostromo Nhttpd Remote Code Execution Vulnerability
Vendor: Nazgul
Description: A Directory Traversal vulnerability exists in the function http_verify in nostromo nhttpd. It allows an attacker to achieve remote code execution via a crafted HTTP request. An attacker can bypass a check for /../ which allows to execute /bin/sh with arbitrary arguments.
CVSS v2 Base Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

ID: CVE-2019-2890
Title: Oracle WebLogic Server Vulnerability
Vendor: Oracle
Description: A vulnerability exists in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Easily exploitable vulnerability allows high privileged attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server.
CVSS v2 Base Score: 6.5 (AV:N/AC:L/Au:S/C:P/I:P/A:P)

ID: CVE-2019-17662
Title: ThinVNC Authentication Bypass Vulnerability
Vendor: Cybelsoft
Description: ThinVNC 1.0b1 is vulnerable to arbitrary file read, which leads to a compromise of the VNC server. The vulnerability exists even when authentication is turned on during the deployment of the VNC server. The password for authentication is stored in cleartext in a file that can be read via a ../../ThinVnc.ini directory traversal attack vector.
CVSS v2 Base Score: 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

ID: CVE-2019-11510
Title: Pulse Connect Secure arbitrary file read vulnerability
Vendor: PulseSecure
Description: In Pulse Secure Pulse Connect Secure (PCS) 8.2 before 8.2R12.1, 8.3 before 8.3R7.1, and 9.0 before 9.0R3.4, an unauthenticated remote attacker can send a specially crafted URI to perform an arbitrary file reading vulnerability.
CVSS v2 Base Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVE ID	Publish Date	Update Date	Description
CVE-2019-17613	10/15/2019	10/15/2019	qibosoft 7 allows remote code execution because do/jf.php makes eval calls. The attacker can use the Point Introduction Management feature to supply PHP code to be evaluated. Alternatively, the attacker can access admin/index.php?lfj=jfadmin&action=addjf via CSRF, as demonstrated by a payload in the content parameter.
CVE-2019-17612	10/15/2019	10/15/2019	An issue was discovered in 74CMS v5.2.8. There is a SQL Injection generated by the _list method in the Common/Controller/BackendController.class.php file via the index.php?m=Admin&c=Ad&a=category sort parameter.
CVE-2019-17602	10/15/2019	10/15/2019	An issue was discovered in Zoho ManageEngine OpManager before 12.4 build 124089. The OPMDeviceDetailsServlet servlet is prone to SQL injection. Depending on the configuration, this vulnerability could be exploited unauthenticated or authenticated.
CVE-2019-17601	10/15/2019	10/15/2019	In MiniShare 1.4.1, there is a stack-based buffer overflow via an HTTP CONNECT request, which allows an attacker to achieve arbitrary code execution, a similar issue to CVE-2018-19862 and CVE-2018-19861. NOTE: this product is discontinued.
CVE-2019-17600	10/15/2019	10/15/2019	Intelbras IWR 1000N 1.6.4 devices allows disclosure of the administrator login name and password because v1/system/user is mishandled.
CVE-2019-17595	10/14/2019	10/15/2019	There is a heap-based buffer over-read in the fmt_entry function in tinfo/comp_hash.c in the terminfo library in ncurses before 6.1-20191012.
CVE-2019-17594	10/14/2019	10/15/2019	There is a heap-based buffer over-read in the _nc_find_entry function in tinfo/comp_hash.c in the terminfo library in ncurses before 6.1-20191012.
CVE-2019-17593	10/14/2019	10/15/2019	JIZHICMS 1.5.1 allows admin.php/Admin/adminadd.html CSRF to add an administrator.
CVE-2019-17592	10/14/2019	10/15/2019	The csv-parse module before 4.4.6 for Node.js is vulnerable to Regular Expression Denial of Service. The __isInt() function contains a malformed regular expression that processes large crafted input very slowly. This is triggered when using the cast option.

CVE ID	Publish Date	Update Date	Description
CVE-2019-17583	10/14/2019	10/15/2019	idreamsoft iCMS 7.0.15 allows remote attackers to cause a denial of service (resource consumption) via a query for many comments, as demonstrated by the admincp.php?app=comment&perpage= substring followed by a large positive integer.
CVE-2019-17580	10/14/2019	10/15/2019	tonyy dormsystem through 1.3 allows SQL Injection in admin.php.
CVE-2019-17579	10/14/2019	10/15/2019	SonarSource SonarQube before 7.8 has XSS in project links on account/projects.
CVE-2019-17575	10/14/2019	10/15/2019	A file-rename filter bypass exists in admin/media/rename.php in WBCE CMS 1.4.0 and earlier. This can be exploited by an authenticated user with admin privileges to rename a media filename and extension. (For example: place PHP code in a .jpg file, and then change the file's base name to filename.ph and change the file's extension to p. Because of concatenation, the name is then treated as filename.php.) At the result, remote attackers can execute arbitrary PHP code.
CVE-2019-17574	10/14/2019	10/15/2019	An issue was discovered in the Popup Maker plugin before 1.8.13 for WordPress. An unauthenticated attacker can partially control the arguments of the do_action function to invoke certain popmake_ or pum_ methods, as demonstrated by controlling content and delivery of popmake-system-info.txt (aka the "support debug text file").
CVE-2019-17553	10/14/2019	10/15/2019	An issue was discovered in MetInfo v7.0.0 beta. There is SQL Injection via the admin/?n=tags&c=index&a=doSaveTags URI.
CVE-2019-17552	10/14/2019	10/15/2019	An issue was discovered in idreamsoft iCMS v7.0.14. There is a spider_project.admincp.php SQL injection vulnerability in the 'upload spider project scheme' feature via a two-dimensional payload.
CVE-2019-17538	10/13/2019	10/13/2019	Jiangnan Online Judge (aka jnoj) 0.8.0 has Directory Traversal for file reading via the web/polygon/problem/viewfile?id=1&name=../ substring.