Red Piranha
unified threat management

Threat Intelligence Report

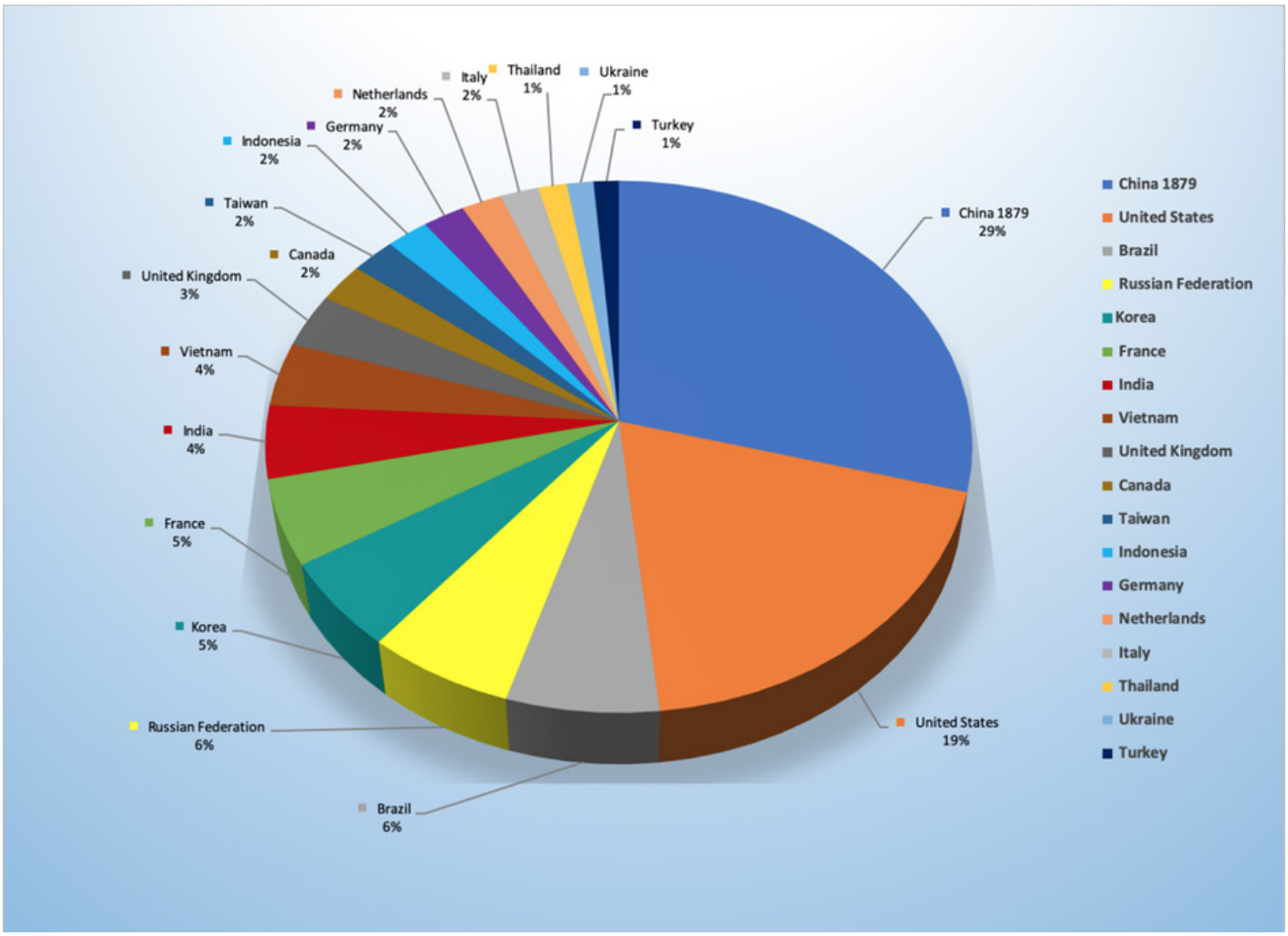
September 16-22, 2019

Trends

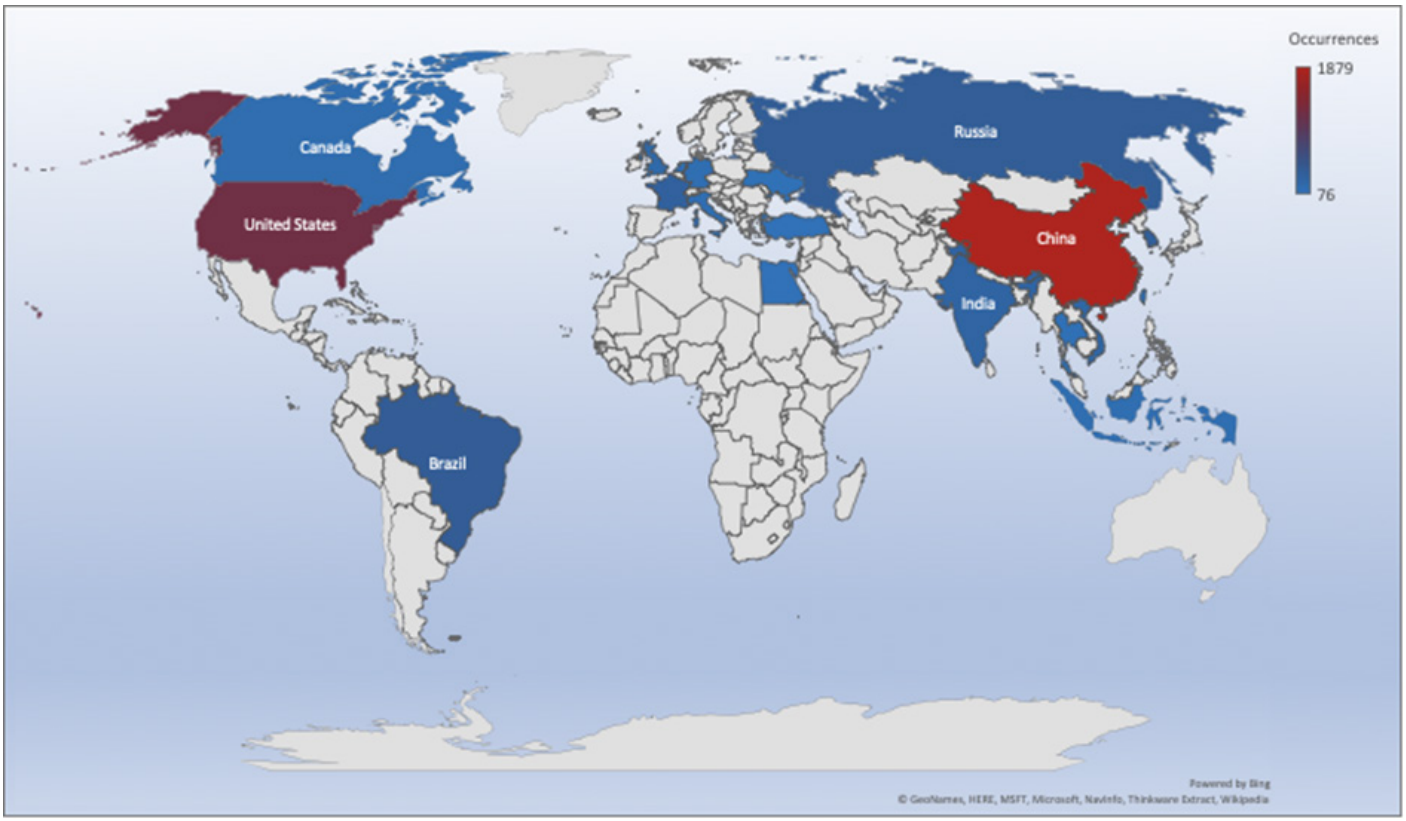
- **The top attacker country was China with 1879 unique attackers (28.89%).**
- **The top Exploit event was Cross Site Scripting with 67% of occurrences.**
- **The top Trojan C&C server detected was TrickBot with 56 instances detected.**

Top Attacker by Country

Country	Occurrences	Percentage
China	1879	28.89%
United States	1227	18.86%
Brazil	411	6.32%
Russian Federation	397	6.10%
Republic of Korea	351	5.40%
France	334	5.13%
India	285	4.38%
Vietnam	249	3.83%
United Kingdom	211	3.24%
Canada	155	2.38%
Taiwan	143	2.20%
Indonesia	137	2.11%
Germany	136	2.09%
Netherlands	130	2.00%
Italy	125	1.92%
Thailand	92	1.41%
Ukraine	86	1.32%
Turkey	81	1.25%
Egypt	76	1.17%

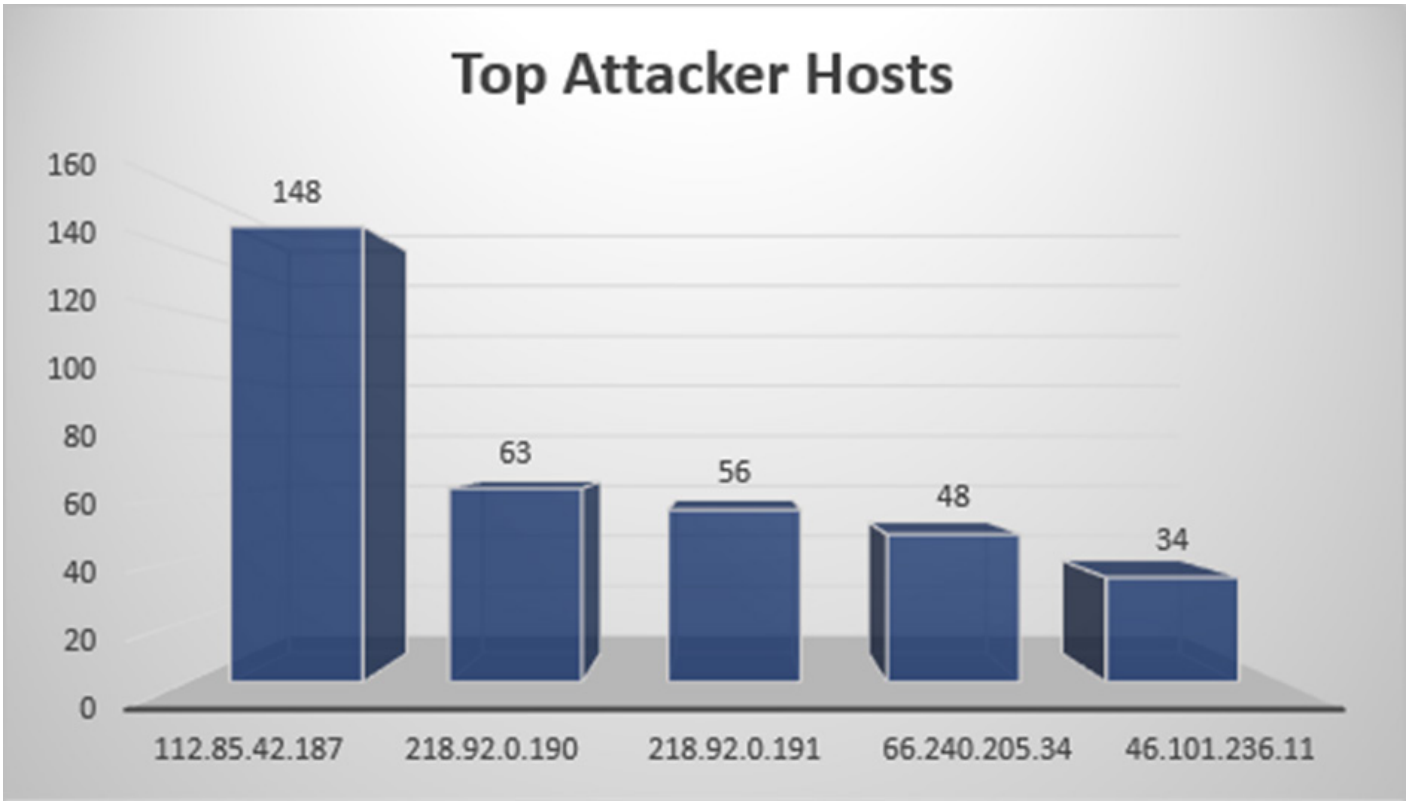


Threat Geo-location



Top Attacking Hosts

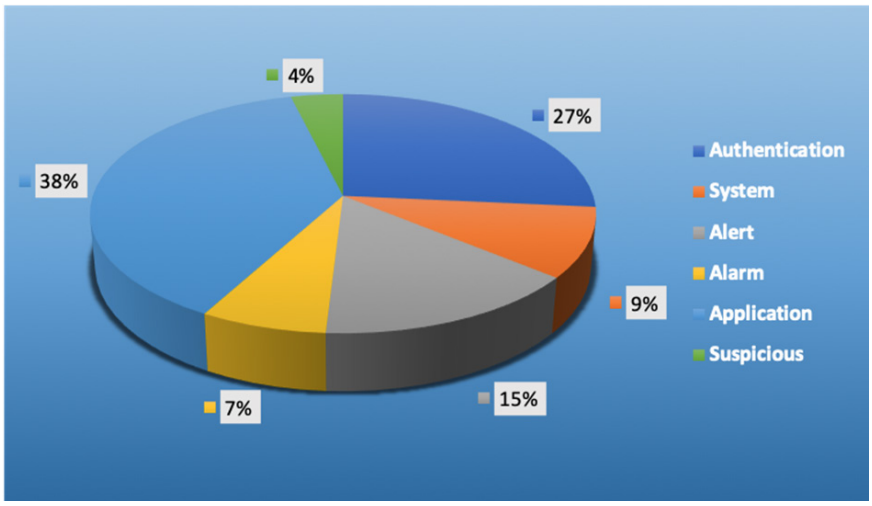
Host	Occurrences
112.85.42.187	148
218.92.0.190	63
218.92.0.191	56
66.240.205.34	48
46.101.236.11	34

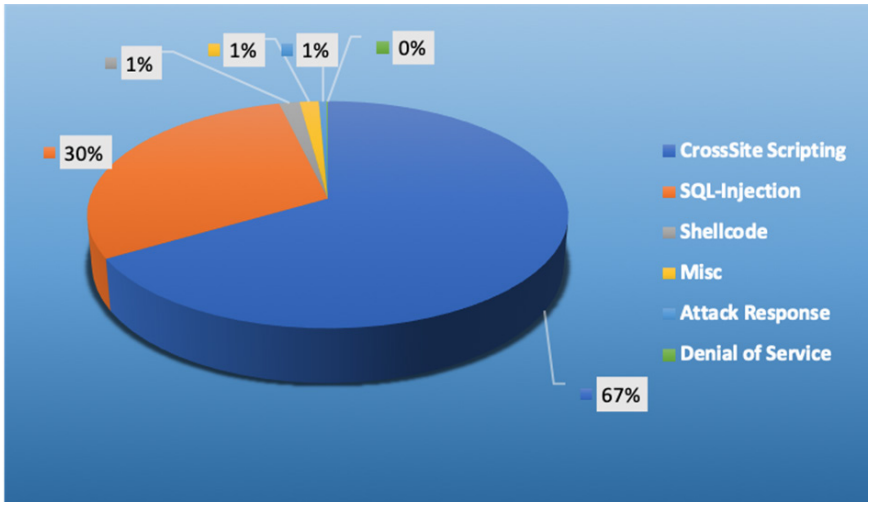


Top Network Attackers

Origin AS	Announcement	Description
AS4837	112.80.0.0/13	China Unicom Jiangsu province network
AS4134	218.92.0.0/16	Chinanet Jiangsu province network
AS14061	46.101.128.0/17	DigitalOcean, LLC

Top Event NIDS and Exploits



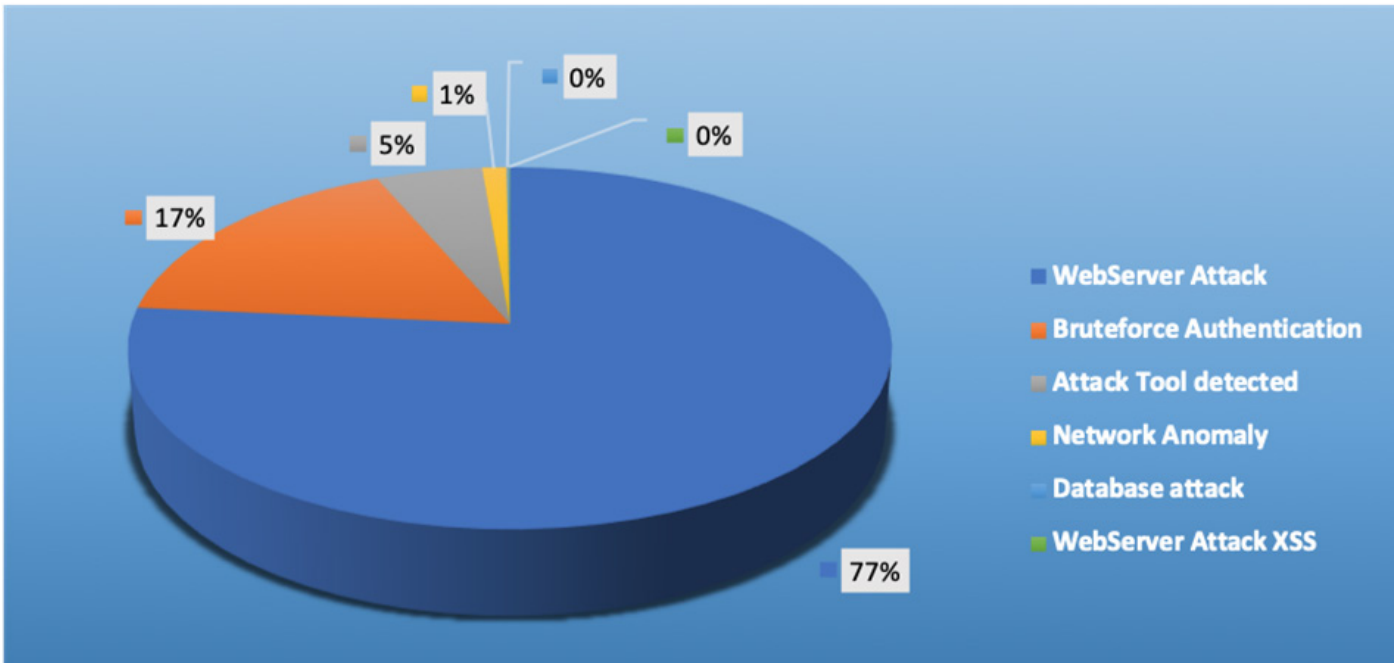


Top Alarms

Type of Alarm	Occurrences
WebServer Attack	1433
Bruteforce Authentication	320
Attack Tool Detected	96
Network Discovery	26
Network Anomaly	22
Database attack	2

Comparison from last week

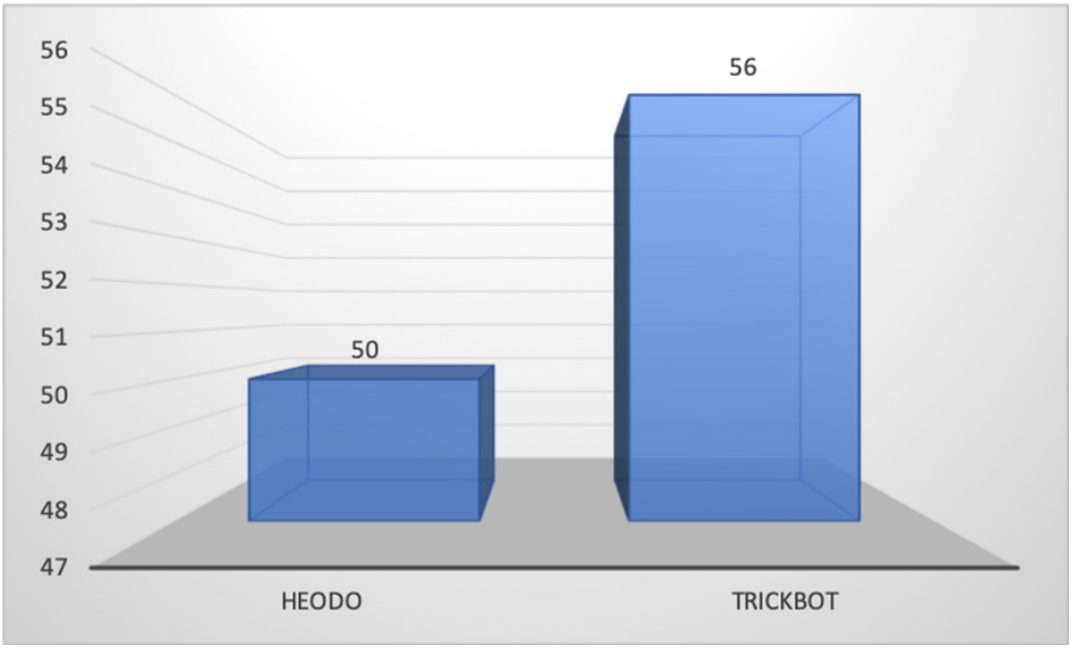
Type of Alarm	Occurrences
Bruteforce Authentication	2598
Intrusion Detection	1387
Network Discovery	922



Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
Heodo	50	133.130.73.156, 62.75.171.248 217.199.160.224, 178.249.187.151 192.241.250.202, 181.164.8.25 181.113.229.139, 95.178.241.254 189.189.214.1, 189.245.216.217 190.79.251.99, 190.104.253.234 46.163.144.228, 62.75.150.240 152.46.8.148, 201.184.65.229 189.129.231.76, 211.229.116.97 63.142.253.122, 158.69.130.55 189.187.141.15, 187.149.84.80 189.166.68.89, 114.79.134.129 187.144.189.58, 187.147.50.167 104.236.243.129, 207.180.208.175 190.55.86.138, 192.163.221.191 181.81.143.108, 189.129.4.186 83.110.75.153, 78.109.34.178 45.33.1.161, 198.199.106.229 190.200.64.180, 190.18.146.70 178.254.6.27, 59.152.93.46 62.210.142.58, 187.155.233.46 201.113.23.175, 200.82.147.93 190.104.64.197, 198.199.88.162 86.98.25.30, 201.250.11.236 179.12.170.88, 181.230.126.152

Name	Number Discovered	Location
TrickBot	56	185.250.204.126, 64.44.133.34 92.63.102.212, 37.228.117.65 145.239.188.95, 195.123.238.36 138.185.25.228, 91.207.185.73 190.152.4.98, 170.233.120.53 170.84.78.117, 178.170.189.239 91.92.128.237, 185.222.202.222 51.68.247.62, 37.44.212.216 23.95.214.138, 93.189.42.21 190.211.254.14, 194.5.250.82 91.132.139.170, 45.8.126.5 46.30.41.229, 212.80.217.164 92.63.102.210, 186.42.98.254 185.70.182.162, 186.42.185.10 45.161.33.88, 181.49.61.237 37.228.117.146, 148.251.185.189 203.23.128.168, 51.254.69.244 213.183.60.30, 79.124.49.215 107.155.137.8, 195.123.221.104 93.189.149.238, 107.173.160.29 31.184.253.37, 108.170.40.39 107.172.143.248, 78.140.223.73 185.117.119.131, 5.53.124.55 195.123.221.178, 185.79.242.204 195.93.223.100, 108.170.40.34 92.38.171.36, 104.193.252.142 185.222.202.62, 194.5.250.79 178.252.26.235, 66.55.71.15



Common Malware

Malware Type	MD5	Typical Filename
W32.7ACF 71AFA8-95. SBX.TG	4a50780 ddb3db1 6ebab57 b0ca42d a0fb	xme64-2141.exe
W32.26DA 22347F-100. SBX.TG	f6f6039f c64ad97 895142d c99554e 971	CSlast.gif
W32.46B2 41E3D3-95. SBX.TG	db69eaa ea4d497 03f161c8 1e6fdd03 6f	xme32-2141-gcc.exe
W32.093C C39350-100. SBX.TG	3c7be1d be9eecfc 73f4476b f18d1df3f	sayext.gif
W32.Generic :Gen.22fz. 1201	799b30f4 7060ca05 d80ece53 866e01cc	mf2016341595.exe

CVEs For Which Public Exploits Have Been Detected

ID: CVE-2019-10669
Title: LibreNMS Collectd Command Injection Vulnerability
Vendor: librenms
Description: A command injection vulnerability exists in html/includes/graphs/device/collectd.inc.php where user supplied parameters are filtered with the mysqli_escape_real_string function. This function is not the appropriate function to sanitize command arguments as it does not escape a number of command line syntax characters such as ` (backtick), allowing an attacker to inject commands into the variable $rrd_cmd, which gets executed via passthru().
CVSS v2 Base Score: 6.5 (AV:N/AC:L/Au:S/C:P/I:P/A:P)

ID: CVE-2019-1245
Title: Microsoft DirectWrite Information Disclosure Vulnerability
Vendor: Microsoft
Description: An information disclosure vulnerability exists when DirectWrite improperly discloses the contents of its memory. Microsoft DirectWrite is a modern Windows API for high-quality text rendering. A majority of its code resides in the DWrite.dll user-mode library. It is used by a variety of widely used desktop programs (such as the Chrome, Firefox and Edge browsers) and constitutes an attack surface for memory corruption bugs, as it performs the processing of untrusted font files and is written in C/C++. There are multiple ways an attacker could exploit the vulnerability, such as by convincing a user to open a specially crafted document, or by convincing a user to visit an untrusted webpage.
CVSS v2 Base Score: 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)

ID: CVE-2019-12922
Title: phpMyAdmin Cross Site Request Forgery Vulnerability
Vendor: phpMyAdmin
Description: A Cross site request forgery issue in phpMyAdmin allows deletion of any server in the Setup page. The attacker can easily create a fake hyperlink containing the request that wants to execute on behalf the user,in this way making possible a CSRF attack due to the wrong use of HTTP method.
CVSS v2 Base Score: 5.8 (AV:N/AC:M/Au:N/C:N/I:P/A:P)

ID: 2019-16173, 2019-16172
Title: LimeSurvey Cross-Site Scripting Vulnerability
Vendor: LimeSurvey
Description: LimeSurvey allows stored cross site scripting for escalating privileges from a low privileged account to, for example, SuperAdmin. The attack uses a survey group in which the title contains JavaScript that is mishandled upon group deletion. By exploiting this vulnerability an attacker could attack other users of the web application with JavaScript code, browser exploits or Trojan horses. An attacker could also perform unauthorized actions in the name of another logged-in user.
CVSS v2 Base Score: 3.5 (AV:N/AC:M/Au:S/C:N/I:P/A:N)

ID: CVE-2019-1253
Title: Microsoft Windows Elevation of Privilege Vulnerability
Vendor: Microsoft
Description: An elevation of privilege vulnerability exists when the Windows AppX Deployment Server improperly handles junctions. To exploit this vulnerability, an attacker would first have to gain execution on the victim system. An attacker could then run a specially crafted application to elevate privileges. AppXSvc improperly handles file hard links resulting in a low privileged user being able to take "Full Control" of an arbitrary file leading to elevation of privilege.
CVSS v2 Base Score: 7.2 (AV:L/AC:L/Au:N/C:C/I:C/A:C)

ID: CVE-2019-10149
Title: Symantec Advanced Secure Gateway Unrestricted File Upload Vulnerability
Vendor: Microsoft
Description: An Unrestricted file upload vulnerability exists in the Symantec Advanced Secure Gateway (ASG) and ProxySG management consoles. A malicious appliance administrator can upload arbitrary malicious files to the management console and trick another administrator user into downloading and executing malicious code.
CVSS v2 Base Score: 6.0 (AV:N/AC:M/Au:S/C:P/I:P/A:P)