Red Piranha
unified threat management

Threat Intelligence Report

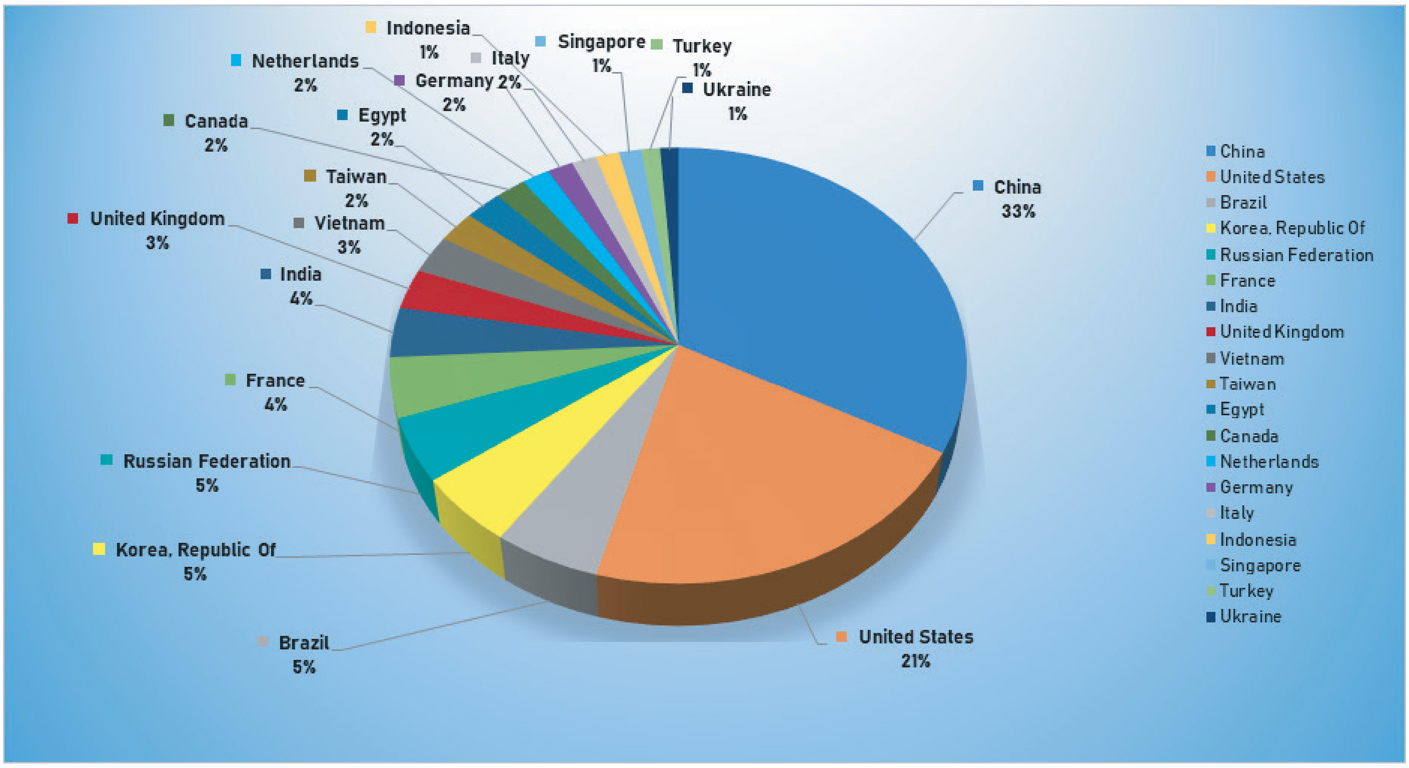
September 9-15, 2019

Trends

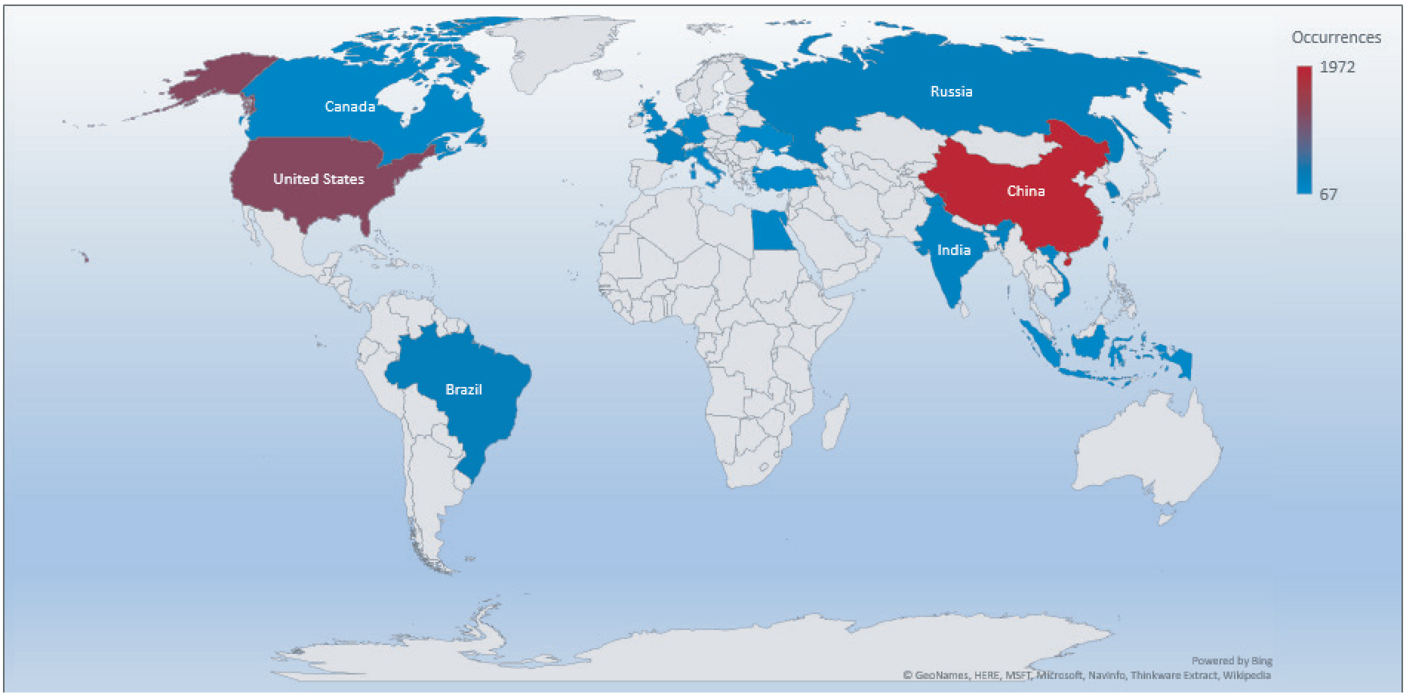
- The top attacker country was China with 1972 unique attackers (33%).
- The top Exploit event was Authentication with 53% of occurrences.
- The top Trojan C&C server detected was TrickBot with 36 instances detected.

Top Attacker by Country

Country	Occurrences	Percentage
China	1471	26.24%
United States	1206	21.51%
Brazil	329	5.50%
Republic of Korea	312	5.21%
Russian Federation	283	4.73%
France	268	4.48%
India	222	3.71%
United Kingdom	178	2.97%
Vietnam	170	2.84%
Taiwan	139	2.32%
Egypt	137	2.29%
Canada	113	1.89%
Netherlands	102	1.70%
Germany	95	1.59%
Italy	90	1.50%
Indonesia	86	1.44%
Singapore	83	1.39%
Turkey	69	1.15%
Ukraine	67	1.12%

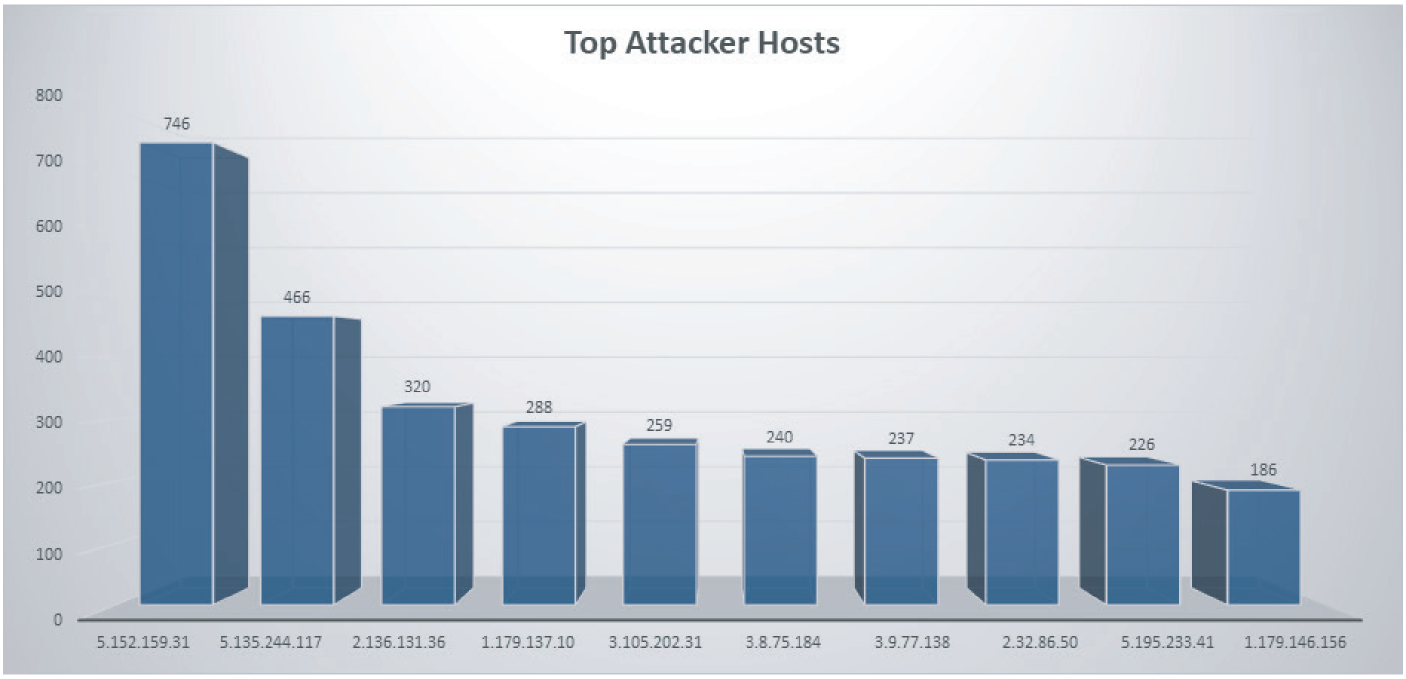


Threat Geo-location



Top Attacking Hosts

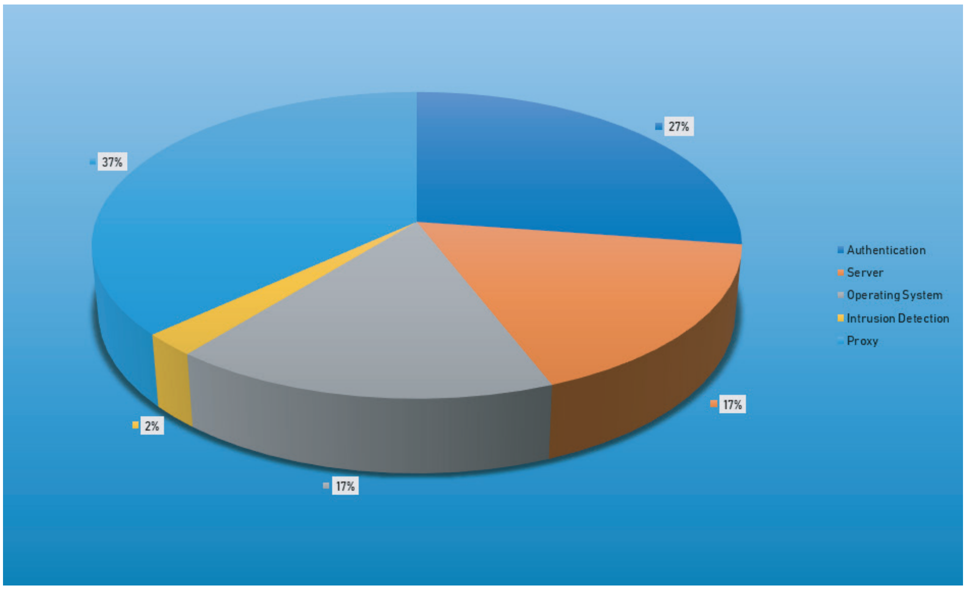
Host	Occurrences
1.34.193.95	837
5.57.33.71	590
1.180.133.42	529
1.223.26.13	416
5.45.73.74	292
3.8.75.184	230
3.9.77.138	230
3.105.202.31	226

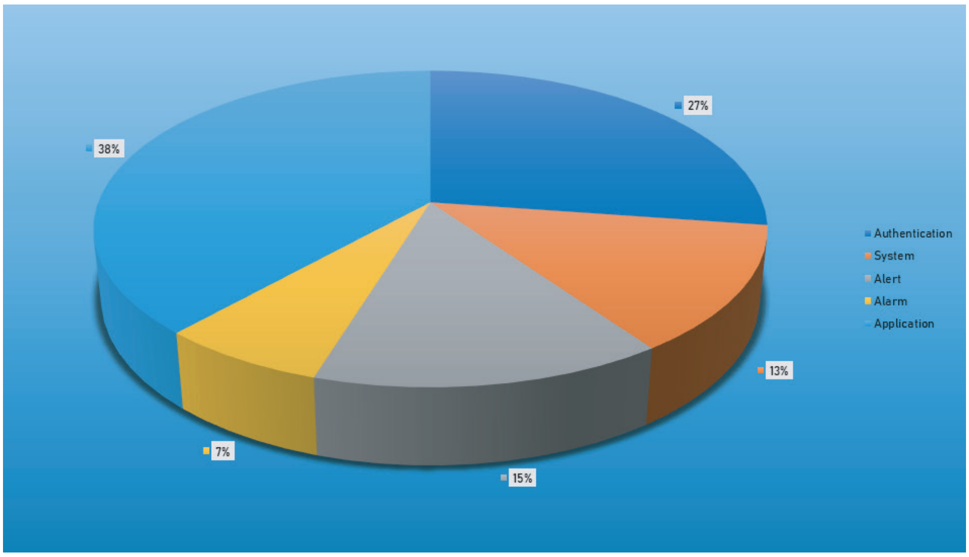


Top Network Attackers

Origin AS	Announcement	Description
AS3462	1.34.0.0/15	Data Communication Business Group
AS3462	5.57.32.0/12	Toloe Rayaneh Loghman Education and Cutural Co.
AS3352	1.180.0.0/14	CHINANET NeiMengGu province network

Top Event NIDS and Exploits



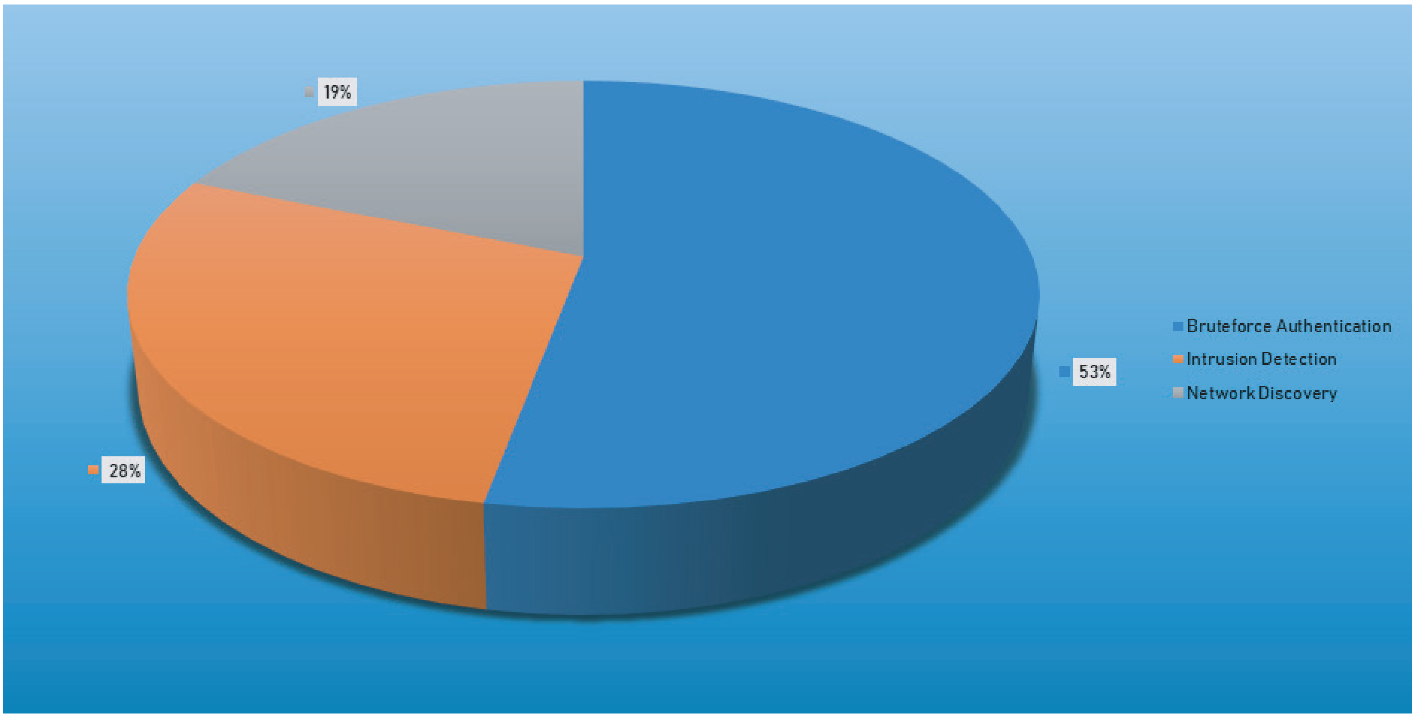


Top Alarms

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

Comparison from last week

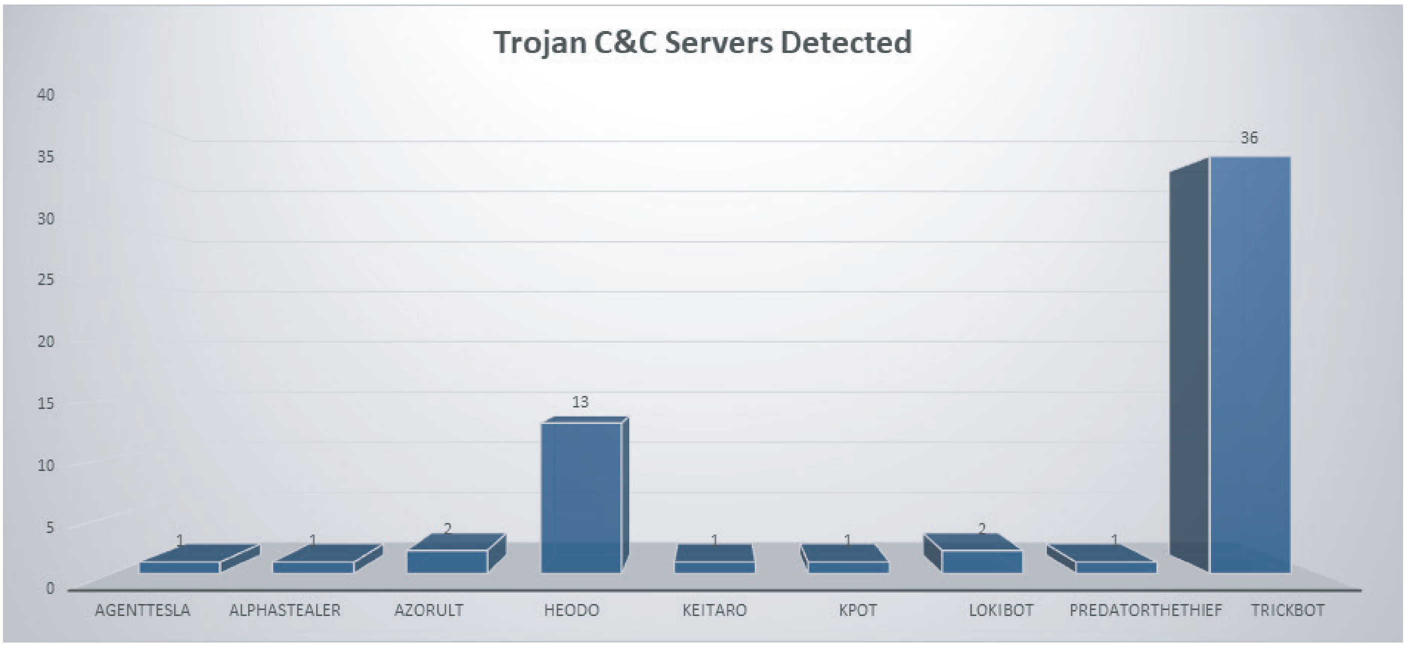
Type of Alarm	Occurrences
Bruteforce Authentication	2294
Network Anomaly	1463
Network Discovery	324



Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
AgentTesla	1	161.117.182.74
AlphaStealer	1	178.208.83.42
Azorult	2	185.173.178.77, 185.224.138.189
Heodo	13	142.44.162.209, 149.202.153.251, 162.241.130.39, 181.188.149.134, 183.82.97.25, 192.241.175.184, 201.212.57.109, 203.130.0.67, 5.67.96.120, 75.127.14.170, 77.245.101.134, 92.222.125.16, 93.78.205.196
keitaro	1	69.16.254.181
Kpot	1	5.188.60.52
LokiBot	2	161.117.182.74 , 47.88.102.244
PredatorTheThief	1	89.41.173.142

Name	Number Discovered	Location
TrickBot	36	104.168.123.186, 107.155.137.4, 107.172.143.155, 139.60.163.36, 148.251.27.94, 178.170.189.52, 178.33.26.175, 181.113.20.186, 181.129.96.74, 185.141.27.223, 185.141.27.237, 185.215.148.133, 185.251.38.201, 185.252.144.190, 185.66.14.149, 186.46.88.62, 194.5.250.57, 194.5.250.60, 195.123.238.110, 195.123.238.83, 195.123.247.27, 198.12.71.210, 200.116.199.10, 200.21.51.38, 200.29.106.33, 23.94.24.196, 37.18.30.165, 37.228.117.182, 5.101.51.101, 51.77.202.8, 51.77.254.186, 64.44.51.126, 79.124.49.209, 79.124.49.210, 92.243.92.8, 92.38.171.26



Common Malware

Malware Type	MD5	Typical Filename
W32.DoublePulsar:WNCryLdrA.22is.1201	c24315b0585b852110977dacafe6c8c1	puls.exe
W32.7ACF71AFA8-95.SBX.TG	4a50780ddb3db16ebab57b0ca42da0fb	xme32-2141.exe
W32.7ACF71AFA8-95.SBX.TG	db69eaaea4d49703f161c81e6fdd036f	xme32-2141-gcc.exe
Win.Trojan.Generic::in10.talos	47b97de62ae8b2b927542aa5d7f3c858	qmreportupload.exe
W32.093CC39350-100.SBX.TG	3c7be1dbe9eecfc73f4476bf18d1df3f	sayext.gif

CVEs For Which Public Exploits Have Been Detected

ID: CVE-2017-1000119
Title: October CMS build 412 PHP code execution Vulnerability
Vendor: Multi-vendor
Description: October CMS build 412 is vulnerable to PHP code execution vulnerability in the file upload functionality resulting in site compromise and possibly other applications on the server. The vulnerability allows an attacker to execute PHP code on a victim's website where the attacker is an authenticated administrator user with media or asset management permissions.
CVSS v2 Base Score: 6.5 (AV:N/AC:L/Au:S/C:P/I:P/A:P)

ID: CVE-2019-15107
Title: LibreNMS Collectd Command Injection Vulnerability
Vendor: Multi-Vendor

Description: LibreNMS is exposed to a command injection vulnerability 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(). An authenticated attacker can execute commands on the server.

CVSS v2 Base Score: 6.5 (AV:N/AC:L/Au:S/C:P/I:P/A:P)

ID: CVE-2019-16118
Title: WordPress Plugin Photo Gallery Cross-Site Scripting Vulnerability
Vendor: Multi-Vendor

Description: WordPress Plugin Photo Gallery is exposed to a cross site scripting (XSS) vulnerability via via admin/controllers/Options.php. This vulnerability occurs whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user supplied data using a browser API that can create JavaScript. The vulnerability allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

CVSS v2 Base Score: 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

ID: CVE-2019-15029
Title: FusionPBX Remote Code Execution Vulnerability
Vendor: Multi-Vendor

Description: FusionPBX allows an attacker to execute arbitrary system commands by submitting a malicious command to the service_edit.php file (which will insert the malicious command into the database). To trigger the command, one needs to call the services.php file via a GET request with the service id followed by the parameter a=start to execute the stored command.

CVSS v2 Base Score: 9.0 (AV:N/AC:L/Au:S/C:C/I:C/A:C)

ID: CVE-2019-11539
Title: Pulse Secure SSL VPN Remote Code Execution Vulnerability
Vendor: Multi-Vendor

Description: In Pulse Secure Pulse Connect Secure and Pulse Policy Secure, the 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.

CVSS v2 Base Score: 6.5 (AV:N/AC:L/Au:S/C:P/I:P/A:P)