Red Piranha
unified threat management

Threat Intelligence Report

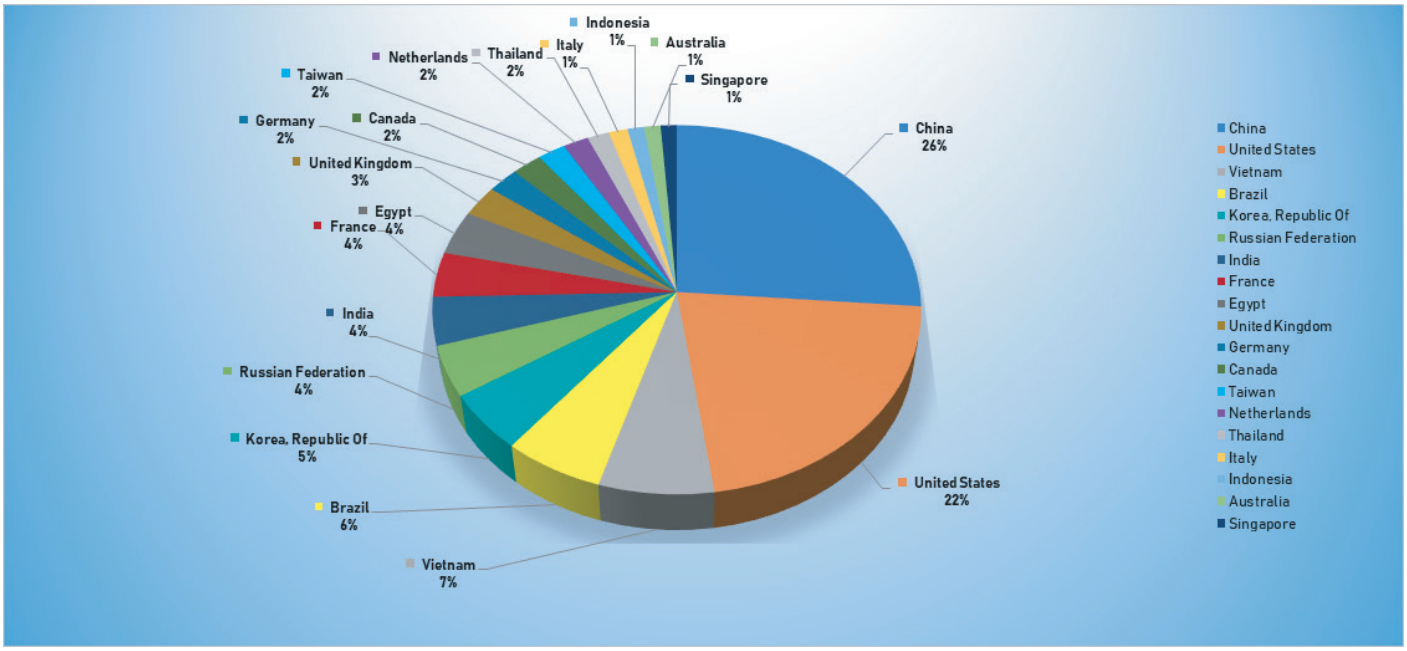
September 2-8, 2019

Trends

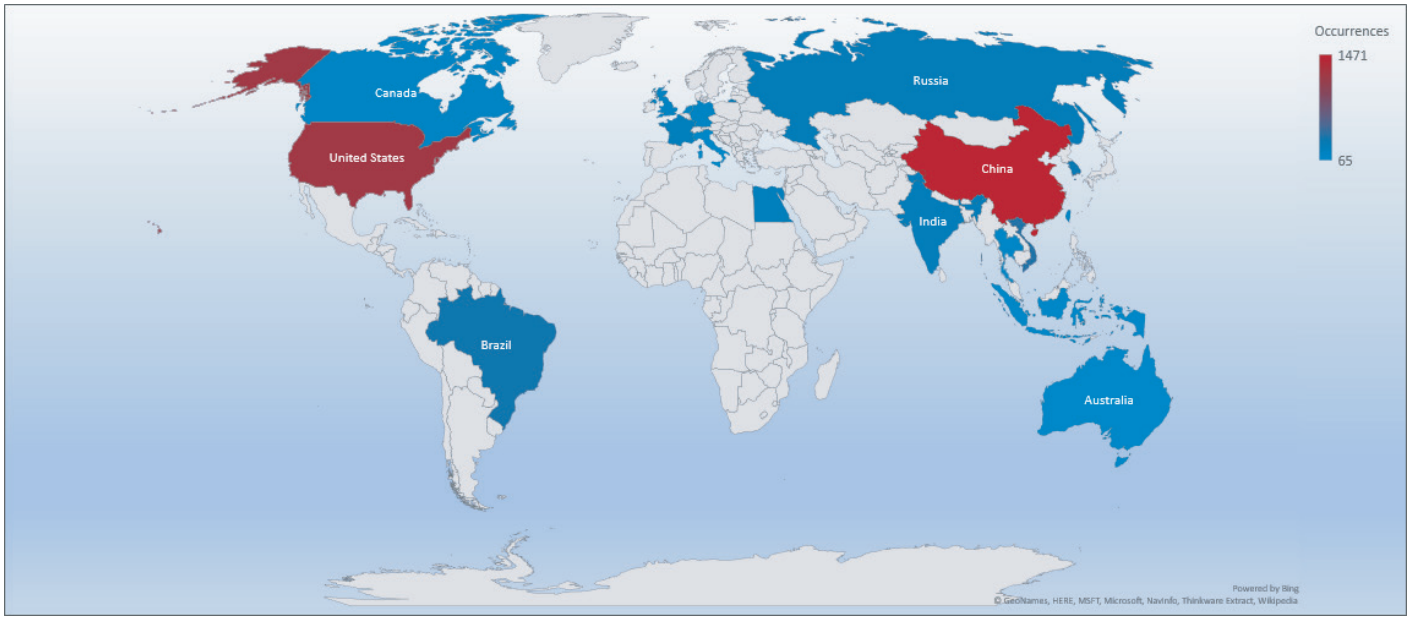
- **The top attacker country was China with 1471 unique attackers (26%).**
- **The top Exploit event was Authentication with 25% of occurrences.**
- **The top Trojan C&C server detected was TrickBot with 32 instances detected.**

Top Attacker by Country

Country	Occurrences	Percentage
China	1673	25.71%
United States	1373	21.10%
Vietnam	357	5.49%
Brazil	343	5.27%
Republic of Korea	330	5.07%
Russian Federation	297	4.56%
India	296	4.55%
Egypt	262	4.03%
United Kingdom	241	3.70%
Germany	235	3.61%
Canada	190	2.92%
Taiwan	182	2.80%
Netherlands	134	2.06%
Thailand	120	1.84%
Italy	113	1.74%
Indonesia	104	1.60%
Australia	93	1.43%
Singapore	87	1.34%

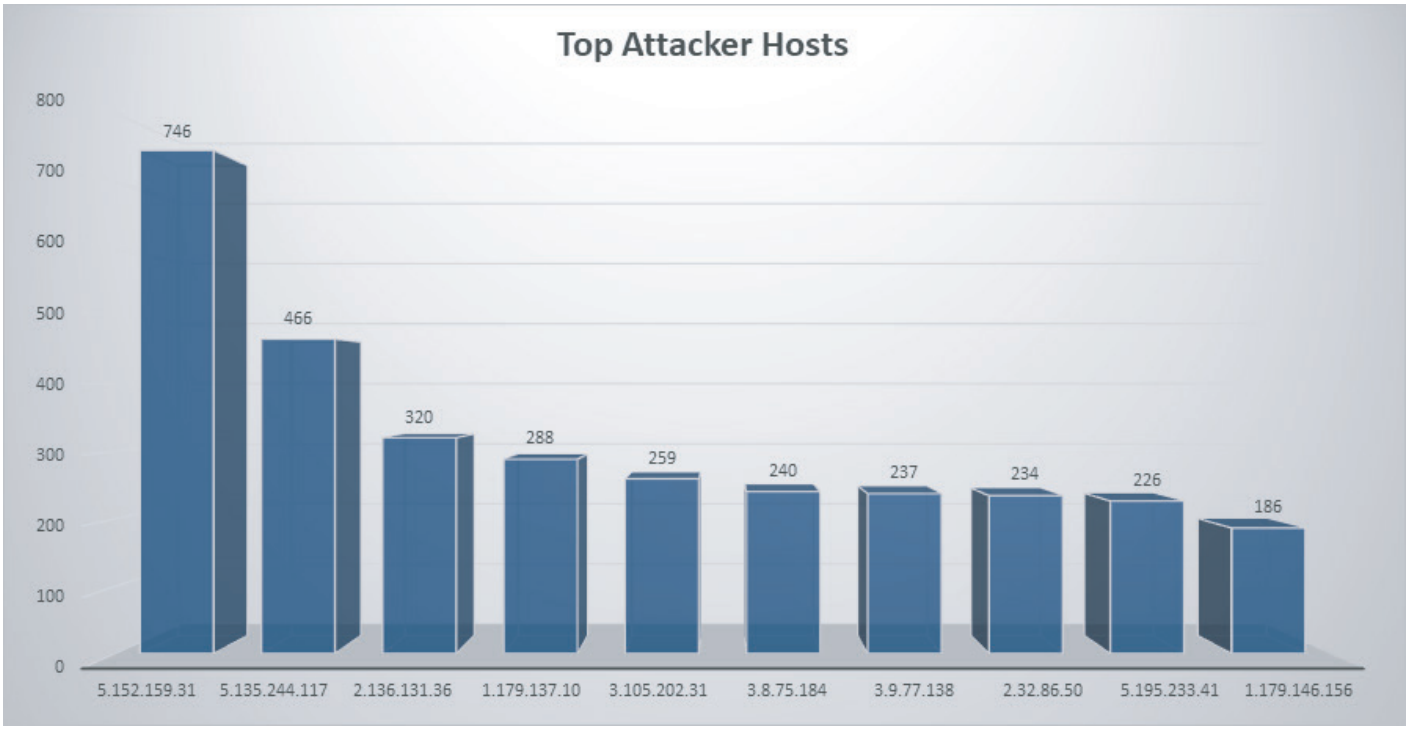


Threat Geo-location



Top Attacking Hosts

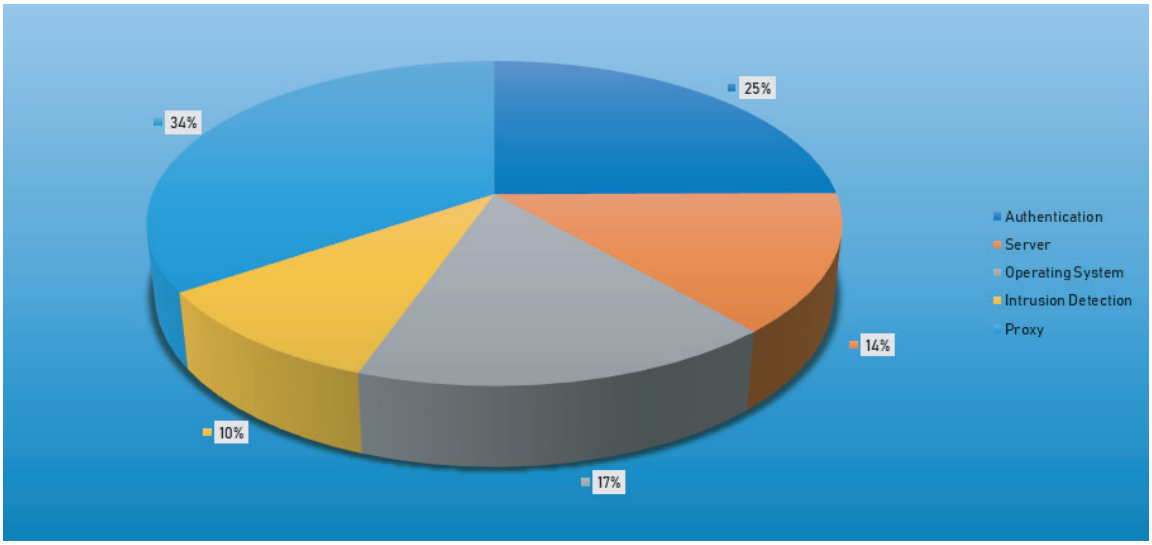
Host	Occurrences
5.152.159.31	746
5.135.244.117	466
2.136.131.36	320
1.179.137.10	288
3.105.202.31	259
3.8.75.184	240
3.9.77.138	237
2.32.86.50	234

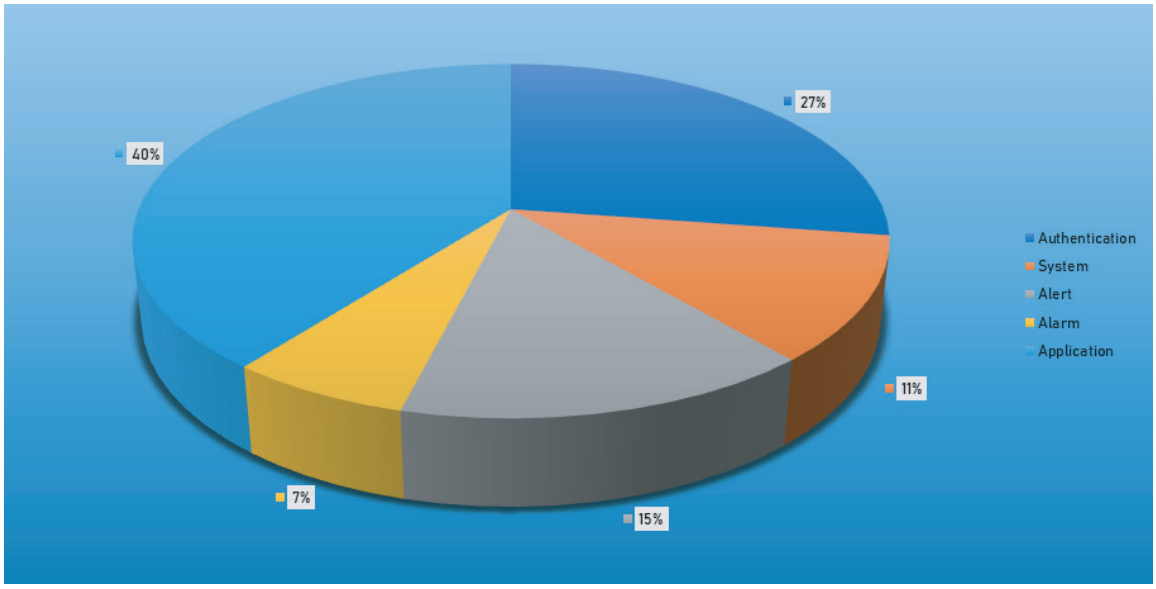


Top Network Attackers

Origin AS	Announcement	Description
AS199026	5.152.159.0/24	alternatYva S.r.l.
AS16276	5.135.0.0/16	OVH SAS
AS3352	2.136.0.0/16	Red de servicios IP

Top Event NIDS and Exploits



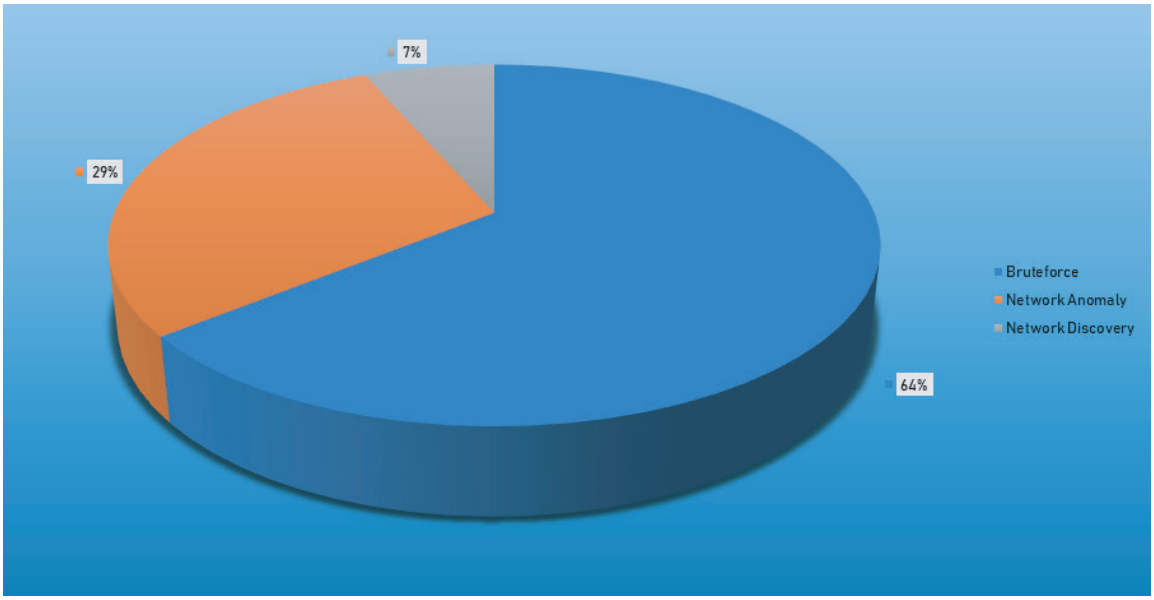


Top Alarms

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

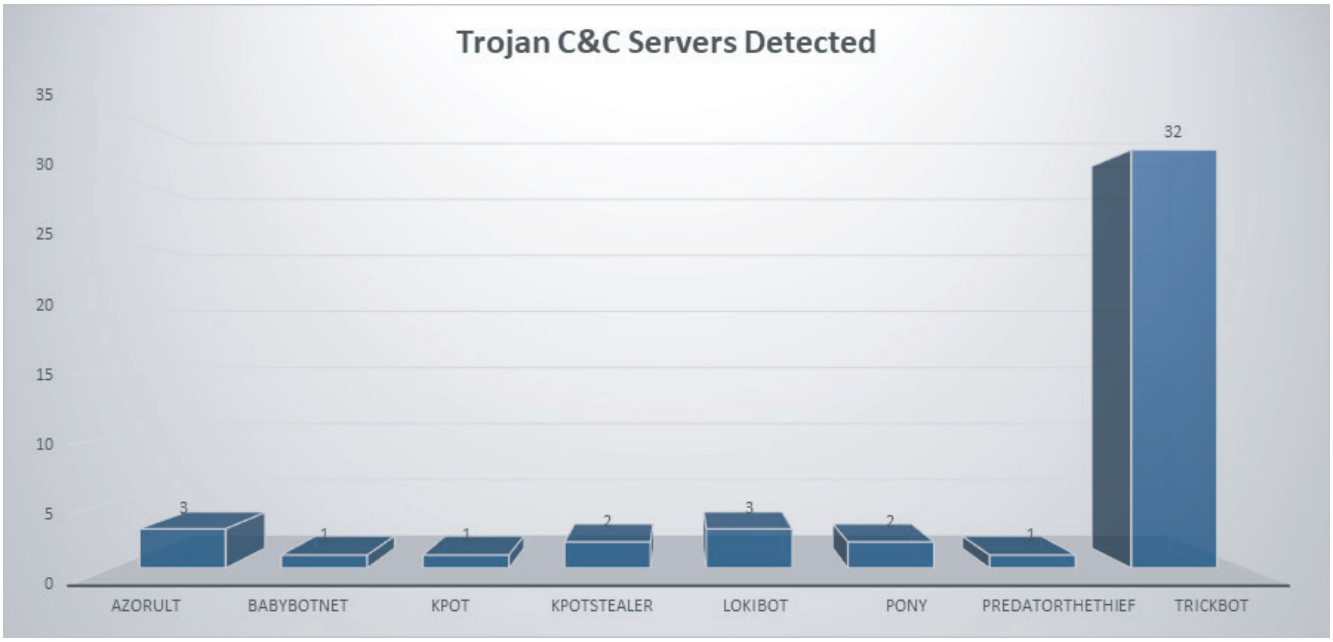
Comparison from last week

Type of Alarm	Occurrences
Bruteforce Authentication	2294
Network Anomaly	2695
Network Discovery	8



Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
Azorult	3	185.213.211.34, 194.67.78.6, 82.202.173.113
BabyBotNet	1	77.222.62.31
KPOT	1	5.188.231.105
KpotStealer	2	47.88.102.244, 8.209.72.105
LokiBot	3	104.24.122.167, 104.27.157.100, 194.67.78.6
Pony	2	104.144.198.27, 116.0.23.168
PredatorTheThief	1	31.184.196.206
TrickBot	32	107.155.137.12, 107.160.141.53, 107.173.160.18, 107.173.160.19, 107.173.160.22, 107.173.90.220, 107.174.66.214, 172.106.131.104, 184.164.142.51, 185.142.99.59, 185.183.99.146, 185.222.202.29, 185.235.130.84, 185.45.193.76, 190.109.189.119, 190.144.89.82, 192.3.104.38, 193.26.217.140, 194.5.250.53, 194.87.147.184, 212.73.150.188, 217.12.210.216, 31.202.132.179, 45.138.157.55, 45.80.148.53, 51.254.69.225, 66.55.71.112, 68.168.123.85, 79.124.49.206, 85.143.216.155, 95.174.65.246, 95.181.198.140



Common Malware

Malware Type	MD5	Typical Filename
Win.Trojan.Generic::in10.talos	47b97de62ae8b2b927542aa5d7f3c858	qmreportupload.exe
W32.9A082883AD-100.SBX.TG	7a6f7f930217521e47c7b8d91fb79649	DHL Scan File.img
W32.7ACF71AFA8-95.SBX.TG	4a50780ddb3db16ebab57b0ca42da0fb	xme64-2141.exe
W32.1755C179F0-100.SBX.TG	c785a8b0be77a216a5223c41d8dd937f	cslast.gif
W32.093CC39350-100.SBX.TG	3c7be1dbe9eecfc73f4476bf18d1df3f	sayext.gif

CVEs For Which Public Exploits Have Been Detected

ID: CVE-2019-0708
Title: Microsoft Remote Desktop Services Remote Code Execution Vulnerability
Vendor: Microsoft
Description: A remote code execution vulnerability exists in Remote Desktop Services – formerly known as Terminal Services – when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability is pre-authentication and requires no user interaction. An attacker who successfully exploited this vulnerability could execute arbitrary code on the target system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.
CVSS v2 Base Score: 10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

ID: CVE-2019-12643
Title: Cisco IOS XE REST API Container Software Authentication Bypass Vulnerability
Vendor: Cisco
Description: This vulnerability resides in the Cisco REST API virtual service container, however, it affects devices running Cisco IOS XE Software when exploited. A successful exploit could allow the attacker to obtain the token-id of an authenticated user. This token-id could be used to bypass authentication and execute privileged actions through the interface of the REST API virtual service container on the affected Cisco IOS XE device. The security issue is tracked as CVE-2019-12643 and has received a maximum severity rating score of 10 based on CVSS v3 Scoring system.
CVSS v2 Base Score: 10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

ID: CVE-2019-1663
Title: Cisco Routers Remote Command Execution Vulnerability
Vendor: Cisco
Description: A vulnerability in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, Cisco RV130W Wireless-N Multifunction VPN Router, and Cisco RV215W Wireless-N VPN Router could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability is due to improper validation of user-supplied data in the web-based management interface. A remote attacker can exploit this issue to execute arbitrary commands on the host operating system with escalated privileges.
CVSS v2 Base Score: 10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

ID: CVE-2019-1622
Title: Cisco Data Center Network Manager Information Disclosure Vulnerability
Vendor: Cisco
Description: A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to retrieve sensitive information from an affected device. The vulnerability is due to improper access controls for certain URLs on affected DCNM software. An attacker could exploit this vulnerability by connecting to the web-based management interface of an affected device and requesting specific URLs. A successful exploit could allow the attacker to download log files and diagnostic information from the affected device.
CVSS v2 Base Score: 5.0 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

ID: CVE-2019-1935
Title: Cisco UCS Director Unauthenticated Remote Access Vulnerability
Vendor: Cisco

Description: A vulnerability in Cisco Integrated Management Controller (IMC) Supervisor, Cisco UCS Director, and Cisco UCS Director Express for Big Data could allow an unauthenticated, remote attacker to log in to the CLI of an affected system by using the SCP User account (scpuser), which has default user credentials. The vulnerability is due to the presence of a documented default account with an undocumented default password and incorrect permission settings for that account. Due to several coding errors, it is possible for an unauthenticated remote attacker with no privileges to bypass authentication and abuse a password change function to inject arbitrary commands and execute code as root. An attacker could exploit this vulnerability by using the account to log in to an affected system. A successful exploit could allow the attacker to execute arbitrary commands with the privileges of the scpuser account.

CVSS v2 Base Score: 10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

ID: CVE-2019-15637
Title: Tableau XML External Entity Injection Vulnerability
Vendor: Tableau

Description: Numerous Tableau products are vulnerable to XXE (XML External Entity) vulnerability beacuse of a malicious workbook, extension, or data source, leading to information disclosure or a denial of service vulnerability. This affects Tableau Server, Tableau Desktop, Tableau Reader, and Tableau Public Desktop.

CVSS v2 Base Score: 5.5 (AV:N/AC:L/Au:S/C:P/I:N/A:P)

ID: CVE-2019-10149
Title: Exim Remote Command Execution Vulnerability
Vendor: Exim

Description: Exim is affected by remote command execution vulnerability. The vulnerability is exploitable instantly by a local attacker, remotely exploit this vulnerability in the default configuration. An attacker must keep a connection to the vulnerable server open for 7 days (by transmitting one byte every few minutes), faster methods may exist. Successful exploitation will lead to remote command execution.

CVSS v2 Base Score: 5.5 (AV:N/AC:L/Au:S/C:P/I:N/A:P)
