Red Piranha
unified threat management

Threat Intelligence Report

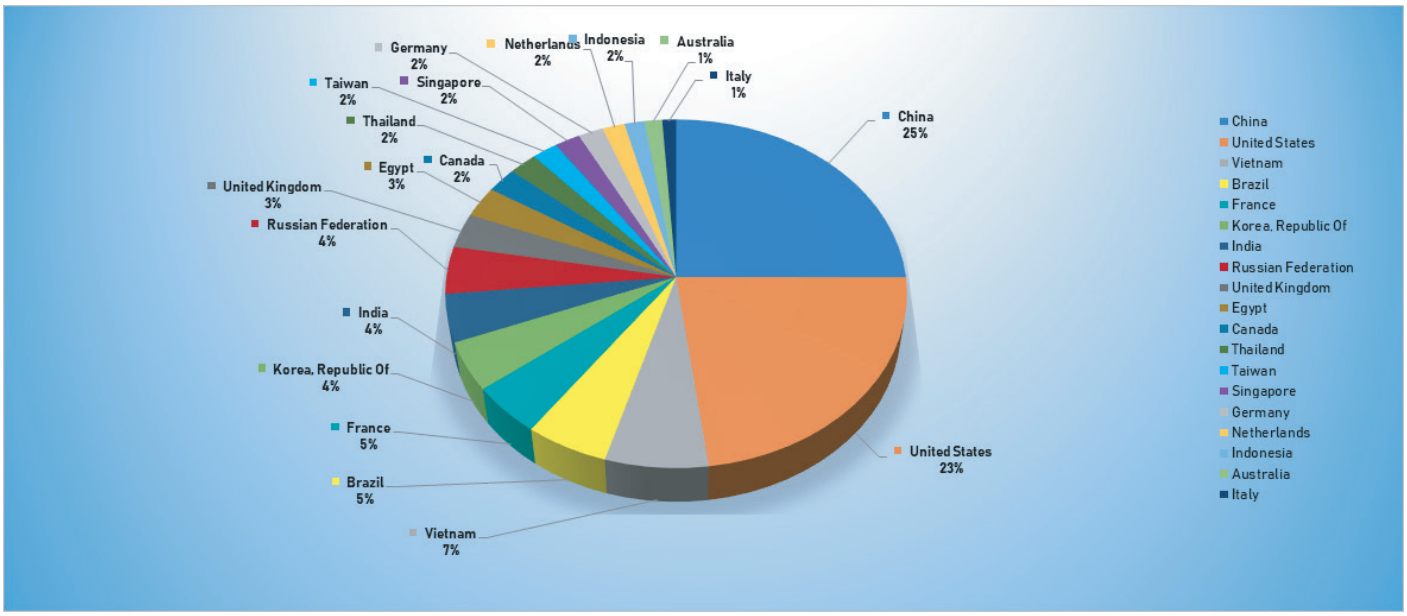
August 26 - September 1, 2019

Trends

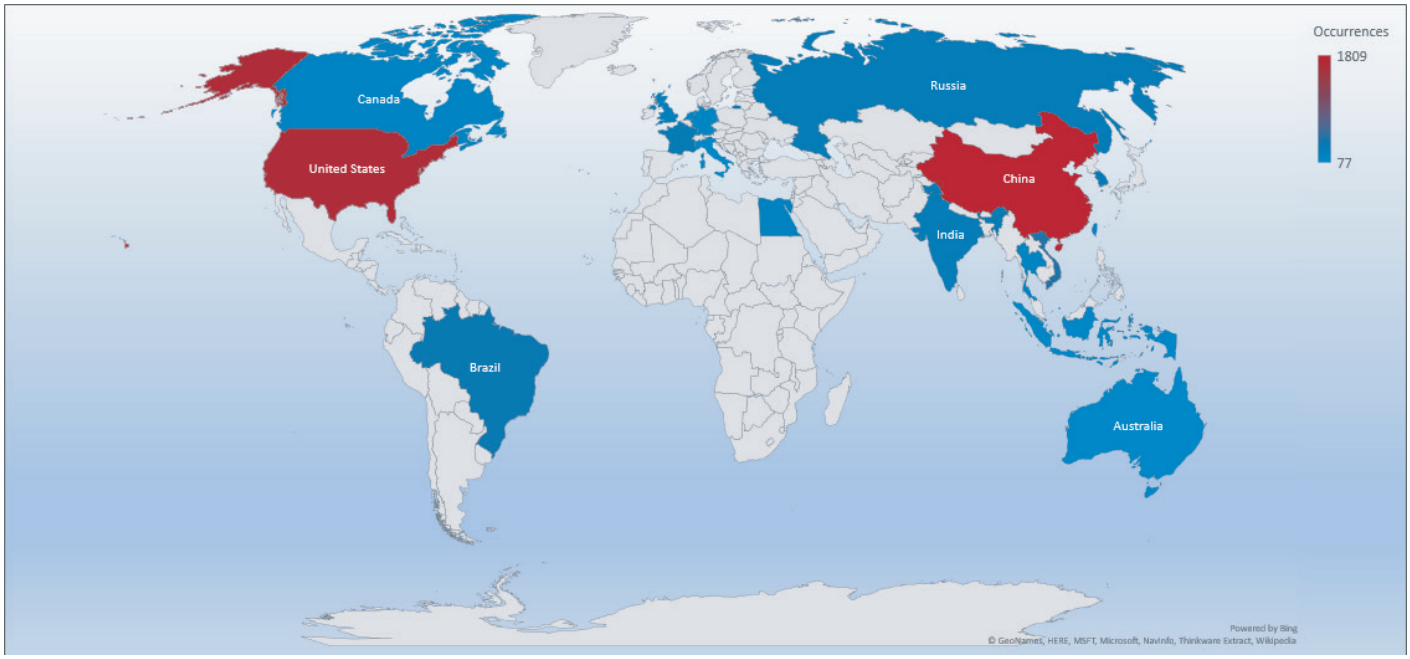
- **The top attacker country was China with 1809 unique attackers (25%).**
- **The top Exploit event was Authentication with 46% of occurrences.**
- **The top Trojan C&C server detected was TrickBot with 21 instances detected.**

Top Attacker by Country

Country	Occurrences	Percentage
China	1809	25.01%
United States	1658	22.93%
Vietnam	478	6.61%
Brazil	386	5.34%
France	336	4.65%
Republic of Korea	325	4.49%
India	321	4.44%
Russian Federation	317	4.38%
United Kingdom	232	3.21%
Egypt	208	2.88%
Canada	170	2.35%
Thailand	157	2.17%
Taiwan	143	1.98%
Singapore	142	1.96%
Germany	140	1.94%
Netherlands	123	1.70%
Indonesia	112	1.55%
Australia	98	1.36%
Italy	77	1.06%

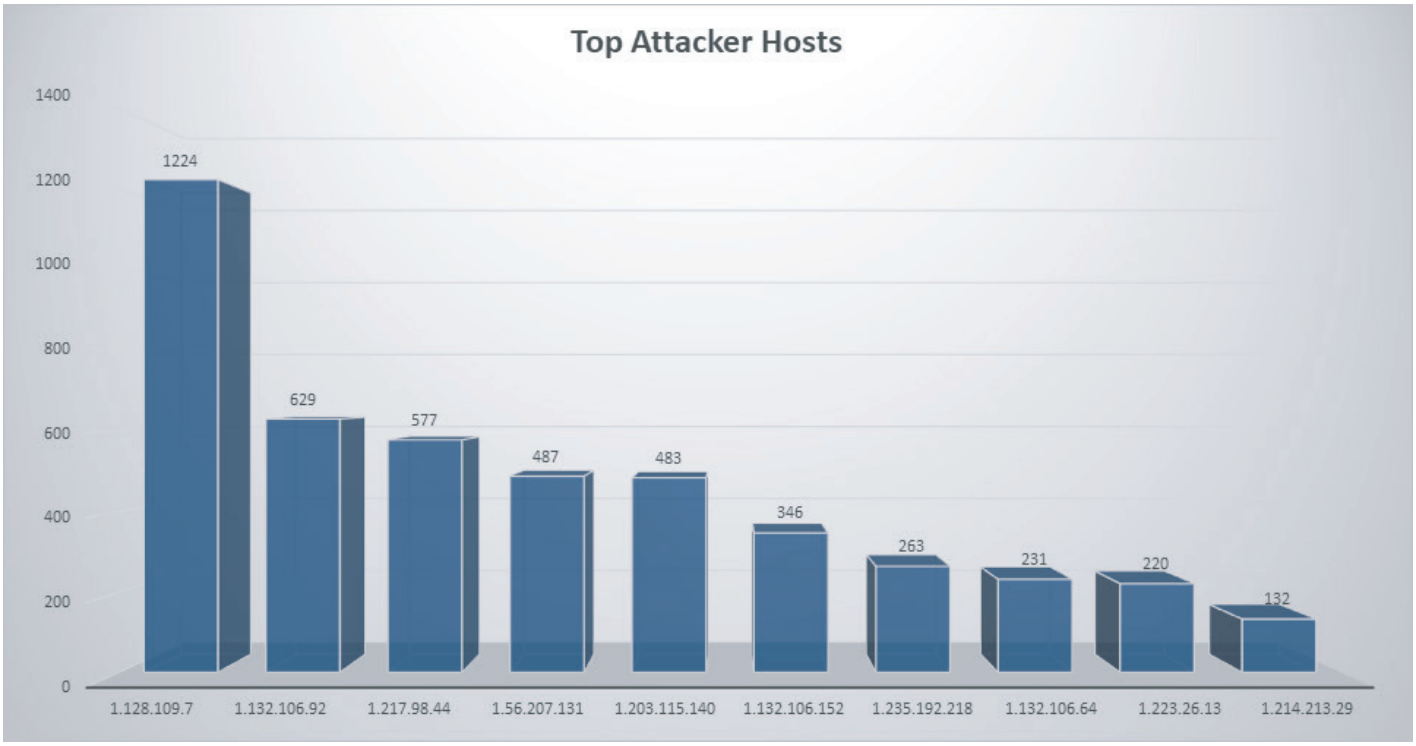


Threat Geo-location



Top Attacking Hosts

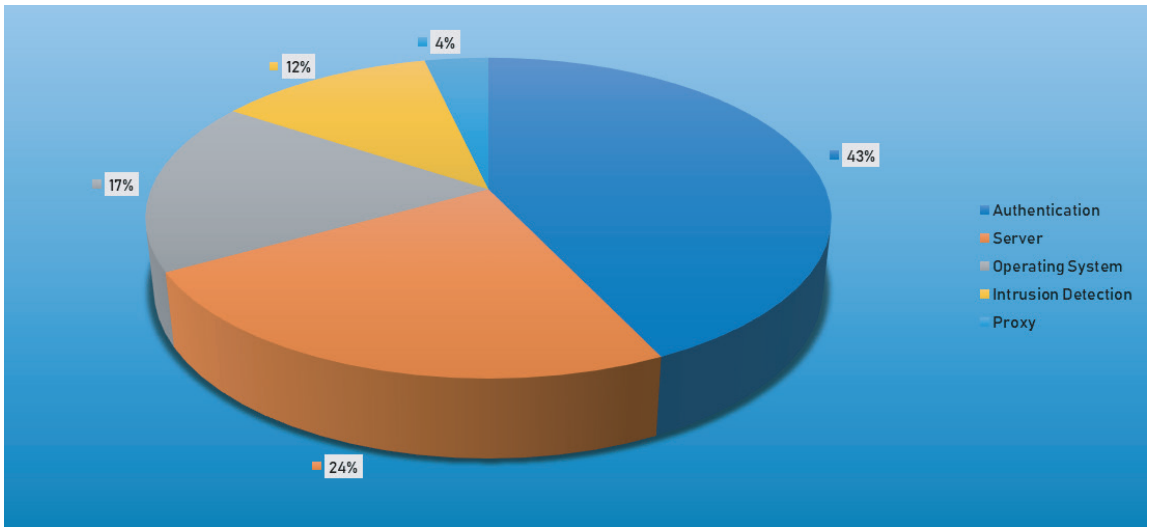
Host	Occurrences
1.128.109.7	1224
1.132.106.92	629
1.217.98.44	577
1.56.207.131	487
1.203.115.140	483
1.132.106.152	346
1.235.192.218	263
1.132.106.64	231

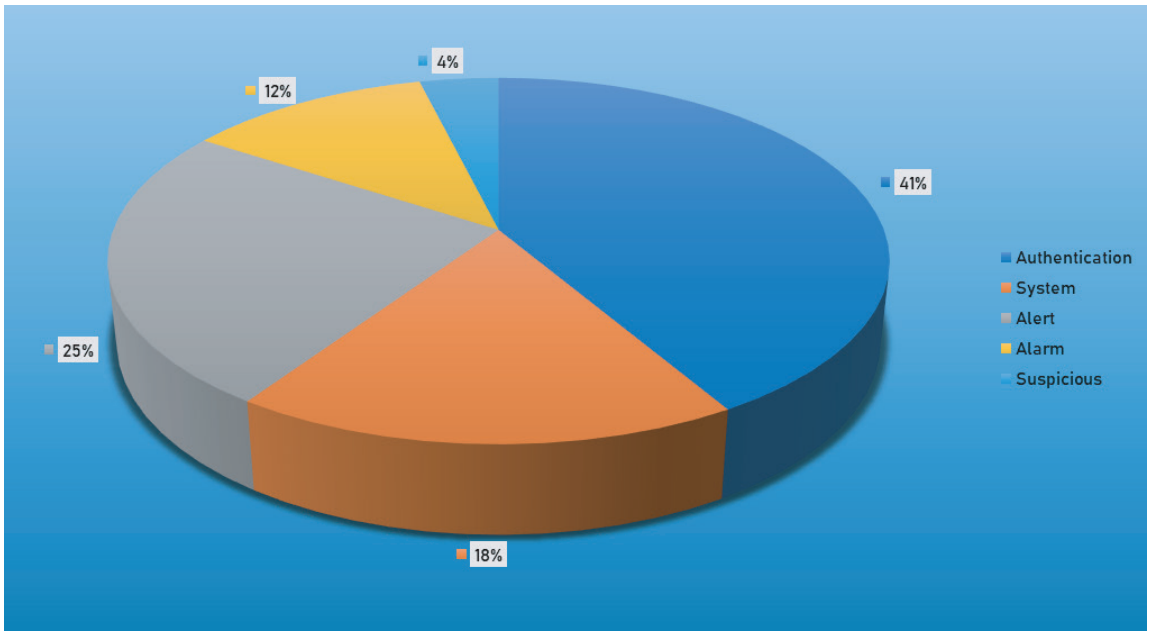


Top Network Attackers

Origin AS	Announcement	Description
AS1221	1.128.0.0/11	Telstra
AS3786	1.208.0.0/12	LG DACOM Corporation
AS4837	1.56.0.0/13	China Unicom Heilongjiang province net

Top Event NIDS and Exploits



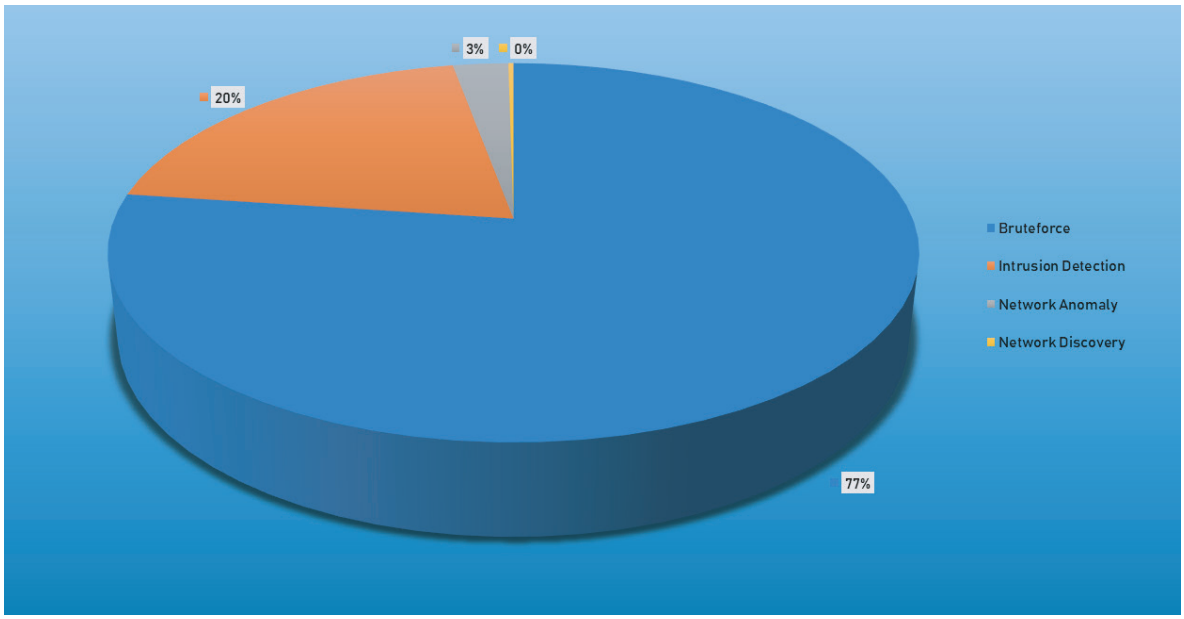


Top Alarms

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

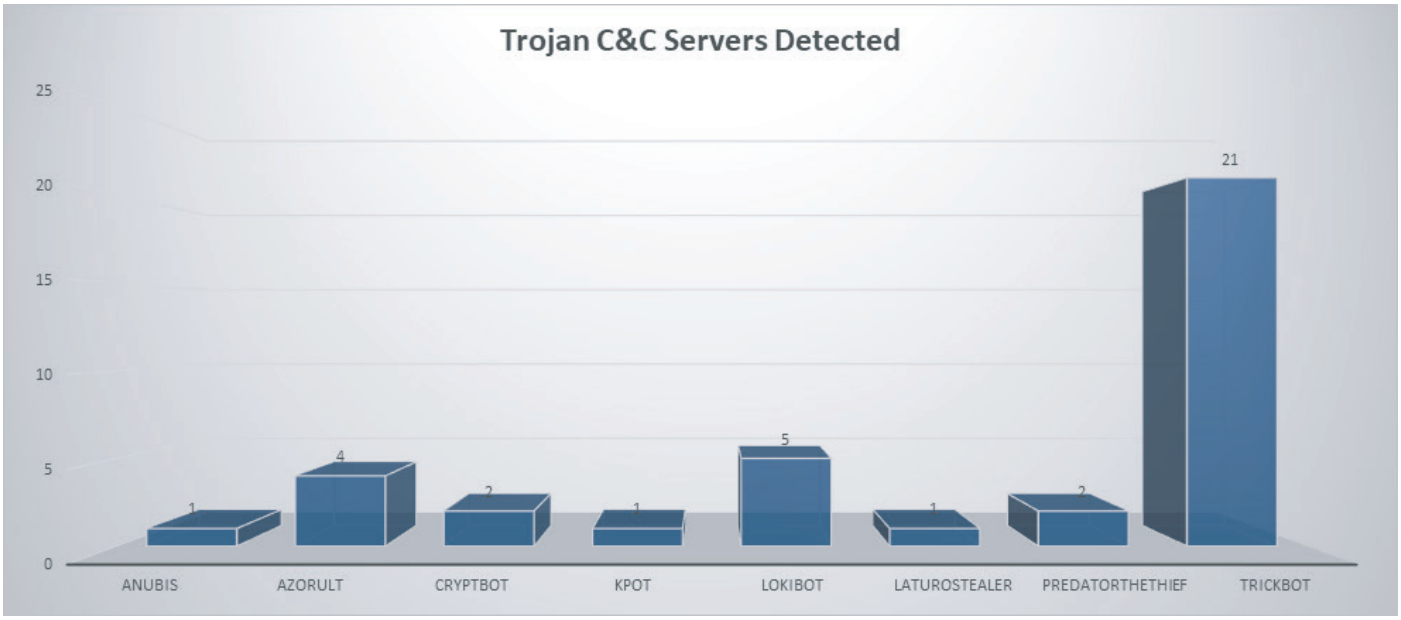
Comparison from last week

Type of Alarm	Occurrences
Bruteforce Authentication	3846
Network Discovery	995
Network Anomaly	131



Remote Access Trojan C&C Servers Found

Name	Number Discovered	Location
Anubis	1	130.0.235.205
Azorult	4	176.119.159.153, 62.109.17.122, 194.67.90.196, 47.88.102.244
CryptBot	2	62.173.154.208, 37.140.199.197
Kpot	1	85.143.217.98
LokiBot	5	101.99.90.11, 47.88.102.244, 194.67.90.196, 149.154.69.146, 194.209.228.127
LaturoStealer	1	176.121.14.128
PredatorTheThief	2	185.25.50.227, 47.88.159.181
TrickBot	21	195.123.237.52, 85.217.171.98, 185.183.98.237, 54.38.127.24, 79.124.49.203, 81.177.6.144, 81.177.6.224, 37.72.168.154, 185.183.99.134, 37.228.117.90, 185.65.202.159, 5.101.51.246, 51.75.254.122, 45.138.157.13, 212.22.75.120, 176.103.62.201, 85.143.221.0, 107.174.254.153, 51.68.247.46, 92.38.171.125, 94.156.35.232



Common Malware

Malware Type	MD5	Typical Filename
Win.Trojan.Generic::in10.talos	47b97de62ae8b2b927542aa5d7f3c858	qmreportupload.exe
W32.7ACF71AFA8-95.SBX.TG	4a50780ddb3db16ebab57b0ca42da0fb	xme64-2141.exe
W32.1755C179F0-100.SBX.TG	c785a8b0be77a216a5223c41d8dd937f	cslast.gif
W32.46B241E3D3-95.SBX.TG	db69eaaea4d49703f161c81e6fdd036f	invoice.exe
W32.093CC39350-100.SBX.TG	3c7be1dbe9eecfc73f4476bf18d1df3f	sayext.gif

CVEs For Which Public Exploits Have Been Detected

ID: CVE-2019-11510
Title: Pulse Secure Arbitrary File Disclosure Vulnerability
Vendor: Pulse Secure
Description: Pulse Connect Secure is exposed to arbitrary file disclosure vulnerability. An attacker can exploit these issues to access arbitrary files in the context of the application, write arbitrary files, or can send a specially crafted URI to perform an arbitrary file reading vulnerability.
CVSS v2 Base Score: 6.5 (AV:N/AC:L/Au:S/C:P/I:P/A:P)

ID: CVE-2019-8605
Title: Apple MacOS Information Disclosure Vulnerability
Vendor: Apple
Description: A remote attacker could exploit this vulnerability to cause disclosure of information, unauthorized modification and arbitrary code execution with system privileges. A malicious application may be able to execute arbitrary code with system privileges," reads the advisory published by Apple. "A use after free issue was addressed with improved memory management." The vulnerability was initially reported by Google Project Zero white hacker Ned Williamson, who also published an exploit for iOS 12.2, dubbed "SockPuppet," after the first patch was released.
CVSS v2 Base Score: 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

ID: CVE-2019-12527
Title: Squid Buffer Overflow Vulnerability
Vendor: Squid
Description: Squid is exposed to a heap based buffer overflow vulnerability because the application fails to properly bounds-check user-supplied data before copying it into an insufficiently sized buffer.When checking Basic Authentication with HttpHeader, Squid uses a global buffer to store the decoded data. Squid does not check that the decoded length is not greater than the buffer, leading to a heap-based buffer overflow with user controlled data. Successfully exploiting this issue allow attackers to execute arbitrary code in the context of the affected application.
CVSS v2 Base Score: 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

ID: CVE-2019-15107
Title: Webmin Unauhenticated Remote Command Execution Vulnerability
Vendor: Webmin
Description: Webmin is exposed to a vulnerability that allows remote command execution. The parameter old in password_change.cgi contains a command injection vulnerability. Webmin versions are only vulnerable if changing of expired passwords is enabled. Successful exploitation may allow remote attacker to execute arbitrary commands on target system.
CVSS v2 Base Score: 10.0 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

ID: CVE-2019-15092
Title: Wordpress Plugin Remote code Execution Vulnerability
Vendor: WordPress

Description: Wordpress Plugin is exposed to CSV injection vulnerability. This allows any application user to inject commands as part of the fields of his profile and these commands are executed when a user with greater privilege exports the data in CSV and opens that file on his machine. The webtoffee "WordPress Users & WooCommerce Customers Import Export" plugin 1.3.0 for WordPress allows CSV injection in the user_url, display_name, first_name, and last_name columns in an exported CSV file created by the WF_CustomerImpExpCsv_Exporter class.

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

ID: CVE-2019-11013
Title: Nimble Streamer Directory Traversal Vulnerability
Vendor: Nimble Streamer

Description: Nimble Streamer is exposed to a "../"" directory traversal vulnerability. Successful exploitation could allow an attacker to traverse the file system to access files or directories that are outside of the restricted directory on the remote server.

CVSS v2 Base Score: 4.0 (AV:N/AC:L/Au:S/C:P/I:N/A:N)

ID: CVE-2019-10149
Title: Exim Local Privilege Escalation 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. Improper validation of recipient address in deliver_message() function in /src/deliver.c may lead to remote command execution.

CVSS v2 Base Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
