Red Piranha
unified threat management

Threat Intelligence Report

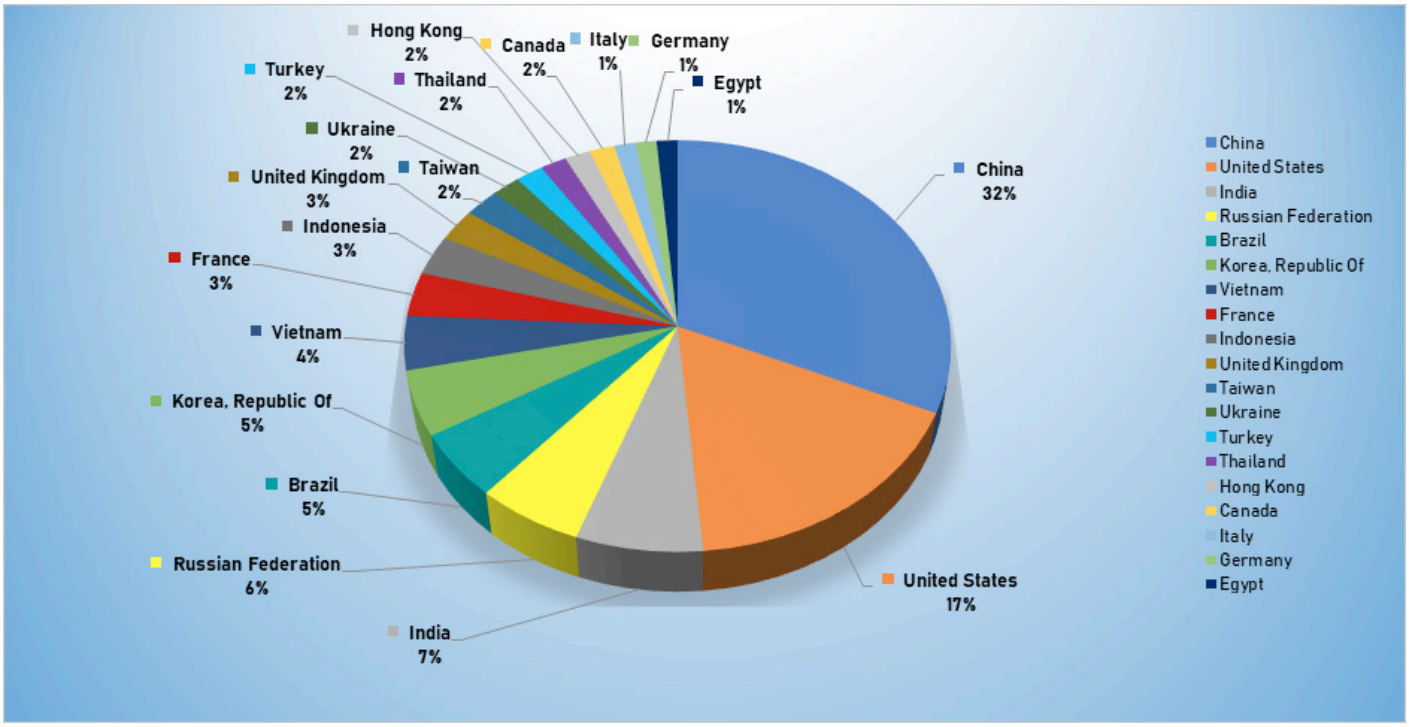
October 7-13, 2019

Trends

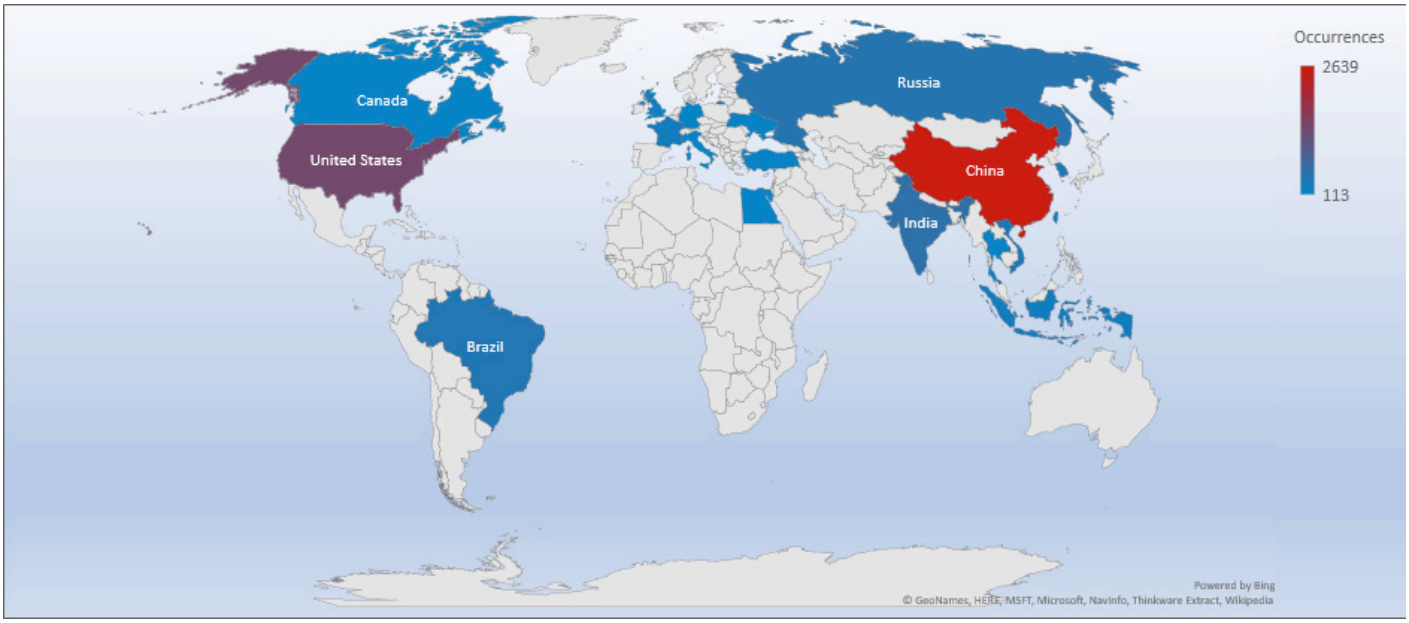
- **The top attacker country was China with 2639 unique attackers (31%)**
- **The top Exploit event was Authentication with 60% of occurrences.**
- **The top Trojan C&C server detected was Trickbot with 43 instances detected.**

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%
Brazil	431	5.18%
Korea	424	5.09%
Vietnam	353	4.24%
France	289	3.47%
Indonesia	262	3.15%
United Kingdom	213	2.56%
Taiwan	190	2.28%
Ukraine	151	1.81%
Turkey	149	1.79%
Thailand	142	1.71%
Hong Kong	139	1.67%
Canada	135	1.62%
Italy	115	1.38%
Germany	114	1.37%
Egypt	113	1.36%

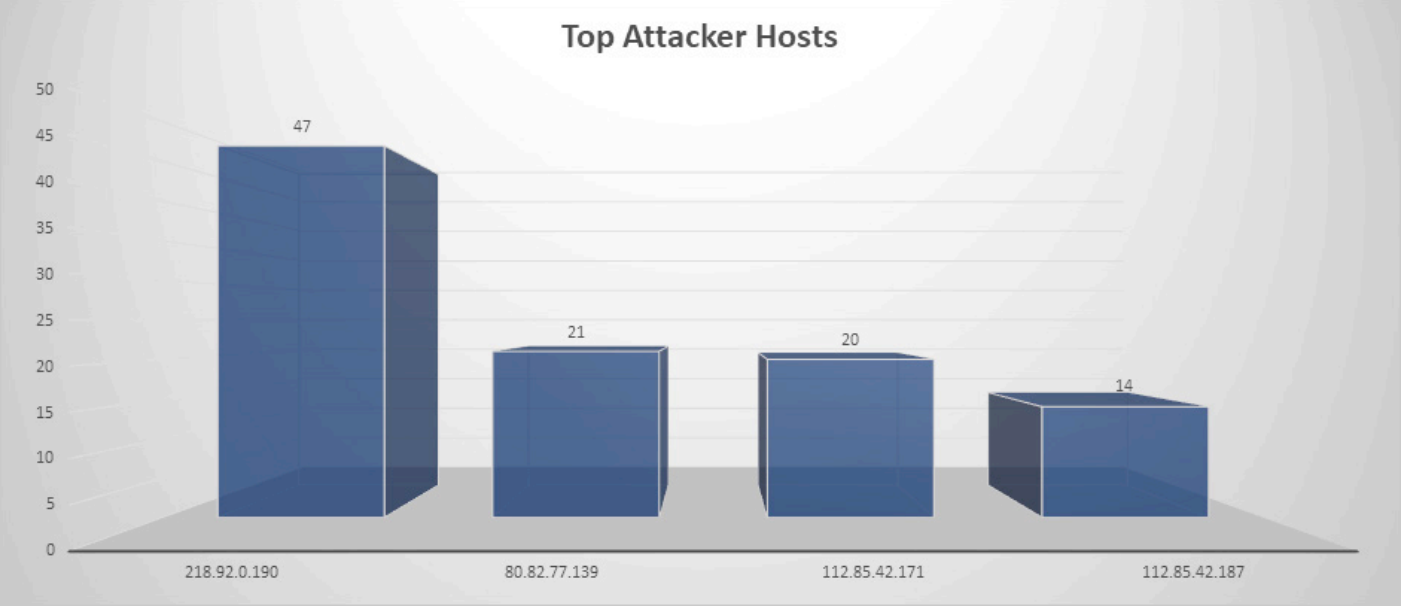


Threat Geo-location



Top Attacking Hosts

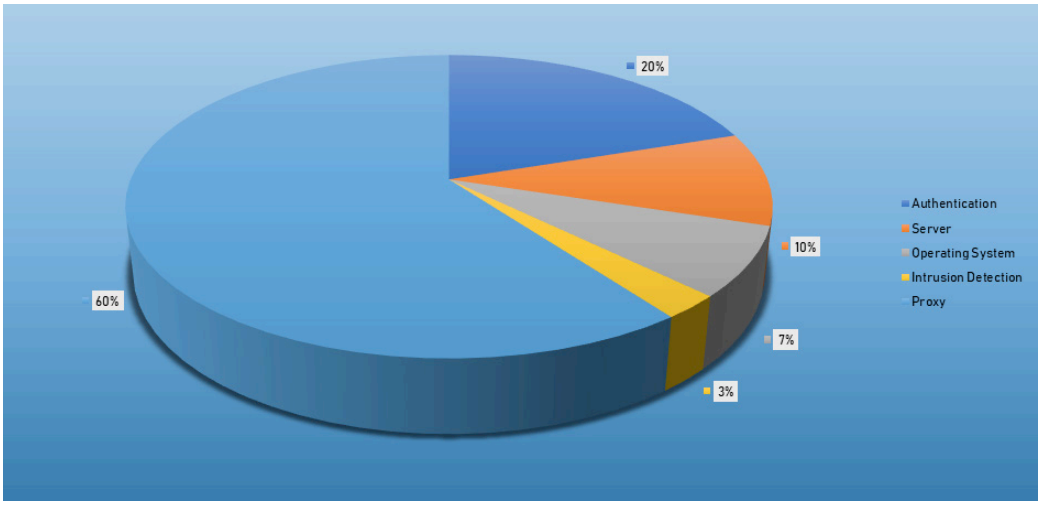
Host	Occurrences
218.92.0.190	47
80.82.77.139	21
112.85.42.171	20
112.85.42.187	14

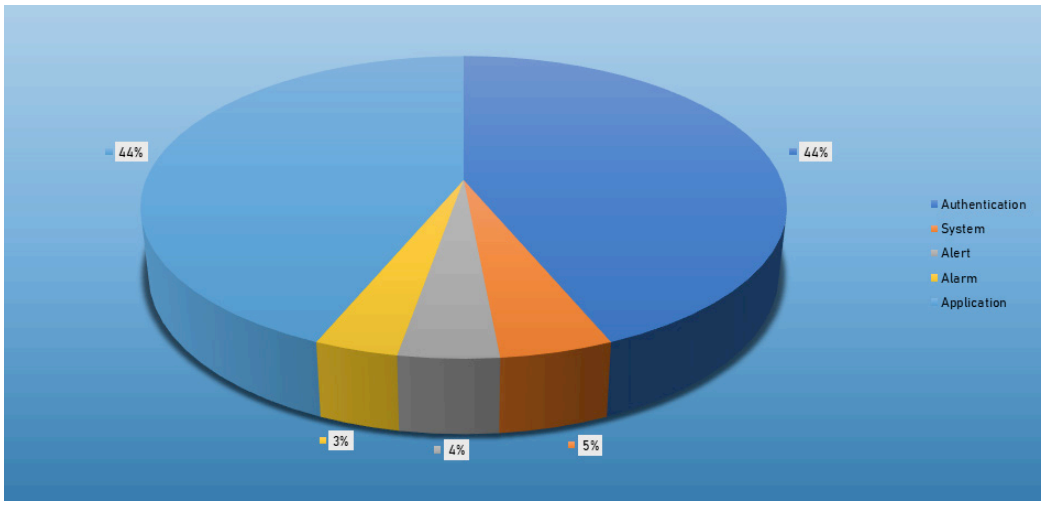


Top Network Attackers

Origin AS	Announcement	Description
AS4134	218.92.0.0/16	CHINANET Jiangsu Province Network
AS202425	80.82.77.0/24	Red de Servicios IP
AS4837	112.80.0.0/13	China Unicom Jiangsu Province Network

Top Event NIDS and Exploits



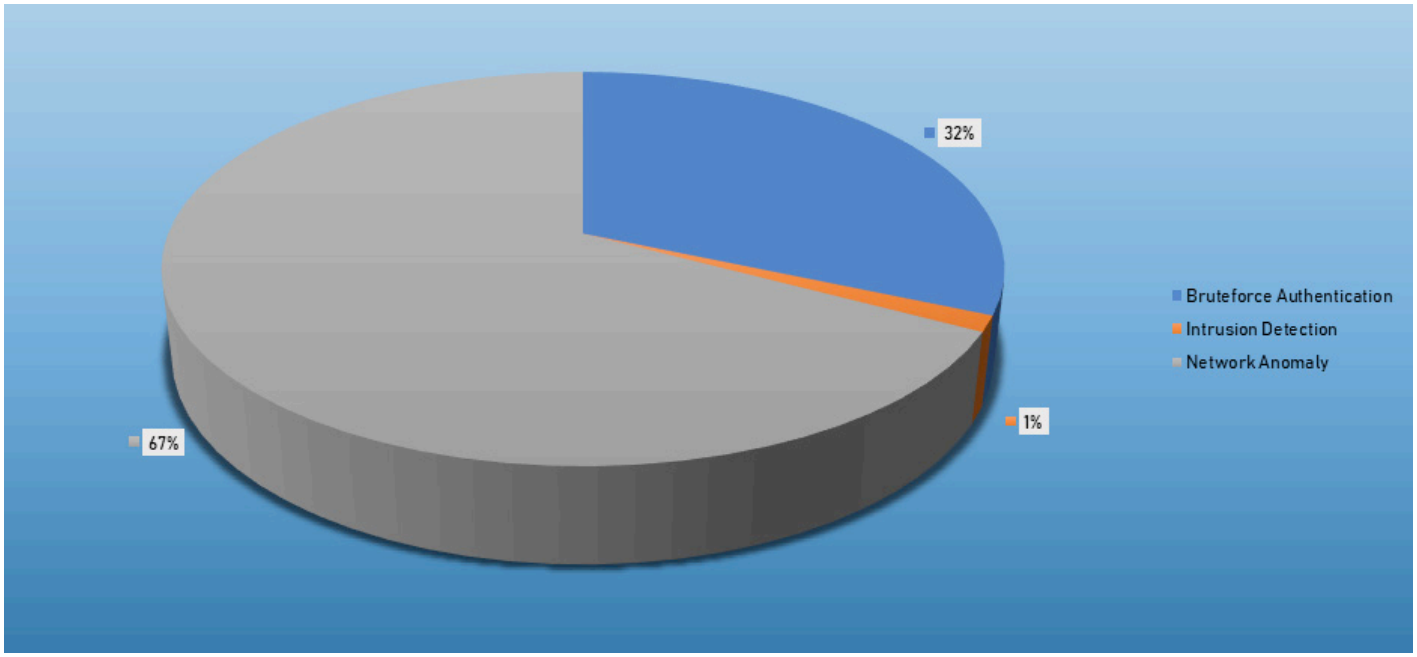


Top Alarms

Type of Alarm	Occurrences
Bruteforce Authentication	808687
Intrusion Detection	33223
Network Discovery	1721987

Comparison from last week

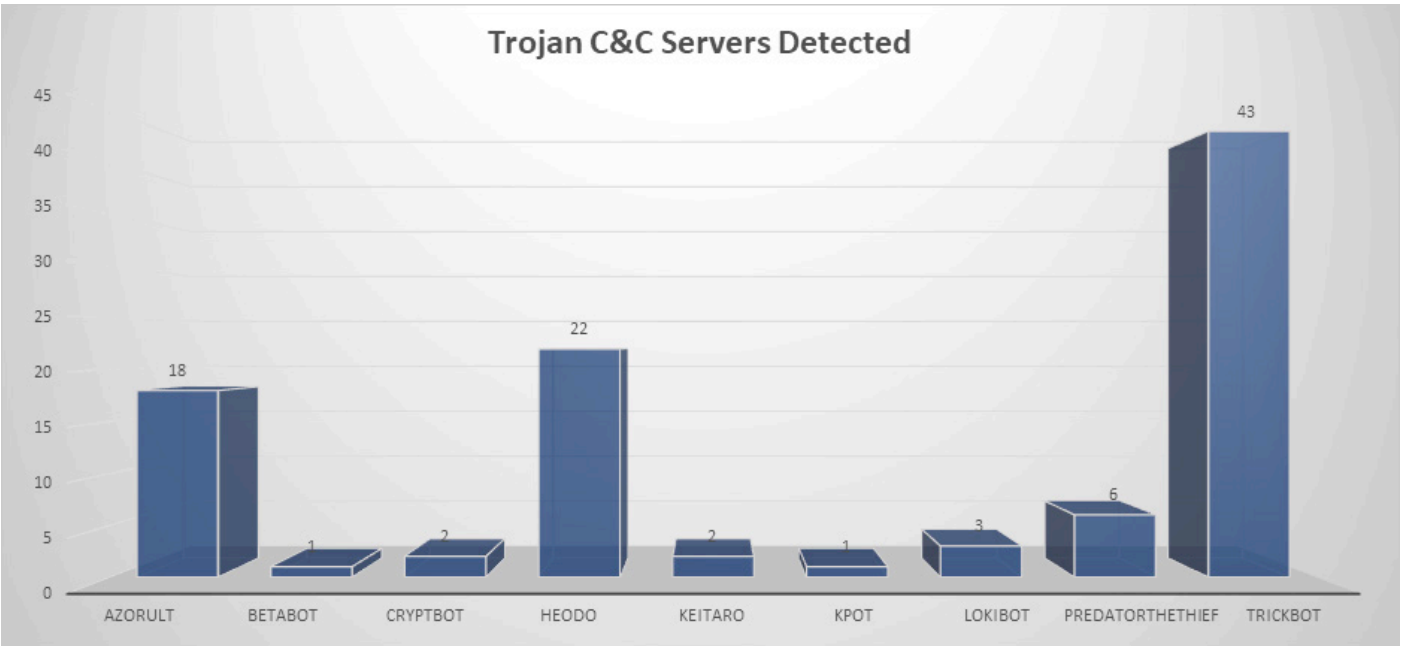
Type of Alarm	Occurrences
Bruteforce Authentication	2035
Intrusion Detection	2879
Network Discovery	20



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	22	133.167.80.63, 144.76.62.10, 173.249.157.58, 179.12.170.88, 181.230.126.152, 181.47.235.26, 187.155.233.46, 189.253.27.123, 198.199.114.69, 198.199.88.162, 201.184.105.242, 201.250.11.236, 203.99.188.203, 213.138.100.98, 216.98.148.181, 23.239.29.211, 24.45.195.162, 68.183.190.199, 70.32.94.58, 86.98.25.30, 91.109.5.28, 91.83.93.105

Name	Number Discovered	Location
Keitaro	2	5.188.231.211, 5.8.88.124
LokiBot	3	194.67.206.57, 47.254.66.50, 91.211.245.184
PredatorTheThief	6	129.226.56.28, 193.124.186.171, 5.188.60.6, 5.8.88.64, 91.243.80.13, 45.128.184.2
TrickBot	43	104.244.76.156, 107.172.248.84, 178.252.26.235, 185.142.99.61, 185.14.31.109, 185.164.32.113, 185.222.202.223, 185.222.202.62, 185.244.150.142, 185.251.38.165, 185.79.243.37, 188.137.81.201, 194.5.250.79, 194.5.250.83, 194.5.250.89, 194.5.250.94, 195.123.220.88, 195.123.247.99, 198.24.134.7, 198.98.51.83, 199.195.254.138, 212.22.75.94, 212.80.216.58, 23.94.233.194, 31.202.132.155, 31.214.138.207, 38.132.99.147, 45.142.213.58, 45.66.11.116, 45.80.148.30, 46.21.153.17, 46.21.153.5, 5.185.67.137, 66.55.71.106, 66.55.71.15, 78.24.217.84, 81.177.26.27, 81.190.160.139, 85.11.116.194, 85.143.218.203, 89.25.238.170, 92.242.40.148, 94.156.144.3



Common Malware

Malware Type	MD5	Typical Filename
Win.Trojan.Generic::in10.talos	47b97de62ae8b2b927542aa5d7f3c858	qmreportupload.exe
W32.7ACF71AFA8-95.SBX.TG	4a5078 0ddb3d b16eba b57b0c a42da0 fb	xme64-2141.exe
W32.CoinMiner:CryptoMinerY.22k3.1201	0e0255 5ede71 bc6c72 4f9f92 4320e0 20	dllhostex.exe
W32.AgentWDCR:Gen.21gn.1201	e2ea31 5d9a83 e75770 53f52c 974f6a 5a	c3e530cc005583b47322b6649ddc0dab1b64bcf22b124a492606763c52fb048f.bin
W32.Generic:Gen.22fz.1201	799b30 f47060 ca05d8 0ece53 866e01 cc	mf2016341595.exe

CVEs For Which Public Exploits Have Been Detected

ID: CVE-2019-11932
Title: Anchor CMS Information Disclosure Vulnerability
Vendor: Anchor CMS
Description: A double free vulnerability in the DDGifSlurp function in decoding.c in libpl_droidsonroids_gif as used in WhatsApp for Android, allows remote attackers to execute arbitrary code or cause a denial of service. By default, AnchorCMS will log errors to the "/anchor/errors.log" file in the webroot of the web application. This allows malicious users to access the error log and view potentially sensitive information.
CVSS v2 Base Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

ID: CVE-2019-1367
Title: Microsoft Scripting Engine Memory Corruption Vulnerability
Vendor: Microsoft

Description: A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. An attacker who successfully exploited the vulnerability could gain the same user rights as the current user. This CVE ID is unique from CVE-2019-1221.

CVSS v2 Base Score: 7.6 (AV:N/AC:H/Au:N/C:C/I:C/A:C)

ID: CVE-2019-1315
Title: Microsoft Windows Error Reporting Privilege Escalation Vulnerability
Vendor: Microsoft

Description: Microsoft Windows could allow a local authenticated attacker to gain elevated privileges on the system, caused by improper handling of hard links by the Error Reporting manager. By executing a specially-crafted program, an authenticated attacker could exploit this vulnerability to take control of the system.

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

ID: CVE-2019-16920
Title: D-Link Unauthenticated Command-Injection Vulnerability
Vendor: D-Link

Description: The vulnerability exists in the latest firmware for the DIR-655, DIR-866L, DIR-652 and DHP-1565 products, which are Wi-Fi routers. The vulnerability exists due to improper sanitization of arbitrary commands that are executed by the native command-execution function. An attacker who successfully triggers the command injection could achieve full system compromise. Fortinet's FortiGuard Labs has discovered an unauthenticated remote code execution vulnerability in D-Link products.

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

ID: CVE-2019-17132
Title: vBulletin Authenticated Remote Code Execution Vulnerability
Vendor: vBulletin

Description: A remote code execution vulnerability exist in User input passed through the "data[extension]" and "data[filedata]" parameters to the "ajax/api/user/updateAvatar" endpoint, that is not properly validated before being used to update users avatars. This can be exploited to inject and execute arbitrary PHP code. Successful exploitation of this vulnerability requires the "Save Avatars as Files" option to be enabled (disabled by default).

CVSS v2 Base Score: 6.4 (AV:N/AC:L/Au:N/C:P/I:N/A:P)

ID: CVE-2019-4013
Title: IBM Bigfix Platform Arbitrary File Upload Vulnerability
Vendor: IBM

Description: IBM BigFix Platform could allow any authenticated user to upload any file to any location on the server with root privileges. This results in code execution on underlying system with root privileges. An attacker can for example upload script file on the web server and execute it by sending GET request.

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

CVE ID	Publish Date	Update Date	Description
CVE-2019-17538	13/10/2019	13/10/2019	Jiangnan Online Judge (aka jnoj) 0.8.0 has Directory Traversal for file reading via the web/polygon/problem/view-file?id=1&name=../ substring.
CVE-2019-17537	13/10/2019	13/10/2019	Jiangnan Online Judge (aka jnoj) 0.8.0 has Directory Traversal for file deletion via the web/polygon/problem/delete-file?id=1&name=../ substring.
CVE-2019-17536	13/10/2019	13/10/2019	Gila CMS through 1.11.4 allows Unrestricted Upload of a File with a Dangerous Type via the moveAction function in core/controllers/fm.php. The attacker needs to use admin/media_upload and fm/move.
CVE-2019-17535	13/10/2019	13/10/2019	Gila CMS through 1.11.4 allows blog-list.php XSS, in both the gila-blog and gila-mag themes, via the search parameter, a related issue to CVE-2019-9647.
CVE-2019-17534	12/10/2019	12/10/2019	vips_foreign_load_gif_scan_image in foreign/gifload.c in libvips before 8.8.2 tries to access a color map before a DGifGetImageDesc call, leading to a use-after-free.
CVE-2019-17533	12/10/2019	12/10/2019	Mat_VarReadNextInfo4 in mat4.c in MATIO 1.5.17 omits a certain '\0' character, leading to a heap-based buffer over-read in strdup_vprintf when uninitialized memory is accessed.
CVE-2019-17532	12/10/2019	12/10/2019	An issue was discovered on Belkin Wemo Switch 28B WW_2.00.11057.PVT-OWRT-SNS devices. They allow remote attackers to cause a denial of service (persistent rules-processing outage) via a crafted ruleDbBody element in a StoreRules request to the upnp/control/rules1 URI, because database corruption occurs.
CVE-2019-17531	12/10/2019	12/10/2019	A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.0.0 through 2.9.10. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has the apache-log4j-extra (version 1.2.x) jar in the classpath, and an attacker can provide a JNDI service to access, it is possible to make the service execute a malicious payload.

CVE ID	Publish Date	Update Date	Description
CVE-2019-17530	12/10/2019	12/10/2019	An issue was discovered in Bento4 1.5.1.0. There is a heap-based buffer over-read in AP4_PrintInspector::AddField in Core/Ap4Atom.cpp when called from AP4_CencSampleEncryption::DoInspect-Fields in Core/Ap4CommonEncryption.cpp, when called from AP4_Atom::Inspect in Core/Ap4Atom.cpp.
CVE-2019-17529	12/10/2019	12/10/2019	An issue was discovered in Bento4 1.5.1.0. There is a heap-based buffer over-read in AP4_CencSampleEncryption::DoInspect-Fields in Core/Ap4CommonEncryption.cpp when called from AP4_Atom::Inspect in Core/Ap4Atom.cpp.
CVE-2019-17528	12/10/2019	12/10/2019	An issue was discovered in Bento4 1.5.1.0. There is a SEGV in the function AP4_TfhdA-tom::SetDefaultSampleSize at Core/Ap4Tfh-dAtom.h when called from AP4_Proces-sor::ProcessFragments in Core/Ap4Proces-sor.cpp.
CVE-2019-17522	12/10/2019	12/10/2019	A stored XSS vulnerability was discovered in Hotaru CMS v1.7.2 via the admin_index-.php?page=settings SITE NAME field (aka SITE_NAME), a related issue to CVE-2011-4709.1.
CVE-2019-17521	12/10/2019	12/10/2019	An issue was discovered in Landing-CMS 0.0.6. There is a CSRF vulnerability that can change the admin's password via the pass-word/ URI,
CVE-2019-17514	12/10/2019	12/10/2019	library/glob.html in the Python 2 and 3 documentation before 2016 has potentially misleading information about whether sorting occurs, as demonstrated by irrepro-ducible cancer-research results. NOTE: the effects of this documentation cross applica-tion domains, and thus it is likely that securi-ty-relevant code elsewhere is affected. This issue is not a Python implementation bug, and there are no reports that NMR research-ers were specifically relying on library/-glob.html. In other words, because the older documentation stated "finds all the pathnames matching a specified pattern according to the rules used by the Unix shell," one might have incorrectly inferred that the sorting that occurs in a Unix shell also occurred for glob.glob. There is a workaround in newer versions of Willough-by nmr-data_compilation-p2.py and nmr-data_compilation-p3.py, which call sort() directly.

CVE ID	Publish Date	Update Date	Description
CVE-2019-17510	11/10/2019	11/10/2019	D-Link DIR-846 devices with firmware 100A35 allow remote attackers to execute arbitrary OS commands as root by leveraging admin access and sending a /HNAP1/ request for SetWizardConfig with shell metacharacters to /squashfs-root/www/HNAP1/control/SetWizardConfig.php.
CVE-2019-17509	11/10/2019	11/10/2019	D-Link DIR-846 devices with firmware 100A35 allow remote attackers to execute arbitrary OS commands as root by leveraging admin access and sending a /HNAP1/ request for SetMasterWLanSettings with shell metacharacters to /squashfs-root/www/HNAP1/control/SetMasterWLanSettings.php.
CVE-2019-17508	11/10/2019	11/10/2019	On D-Link DIR-859 A3-1.06 and DIR-850 A1.13 devices, /etc/services/DEVICE.TIME.php allows command injection via the $SERVER variable.
CVE-2019-17507	11/10/2019	11/10/2019	An issue was discovered on D-Link DIR-816 A1 1.06 devices. An attacker could access management pages of the router via a client that ignores the 'top.location.href = "/dir_login.asp"' line in a .asp file. This provides access to d_status.asp, version.asp, d_dhcptbl.asp, and d_acl.asp.
CVE-2019-17506	11/10/2019	11/10/2019	There are some web interfaces without authentication requirements on D-Link DIR-868L B1-2.03 and DIR-817LW A1-1.04 routers. An attacker can get the router's username and password (and other information) via SERVICES=DEVICE.ACCOUNT&AUTHORIZED_GROUP=1%0a to getcfg.php. This could be used to control the router remotely.
CVE-2019-17505	11/10/2019	11/10/2019	D-Link DAP-1320 A2-V1.21 routers have some web interfaces without authentication requirements, as demonstrated by uplink_info.xml. An attacker can remotely obtain a user's Wi-Fi SSID and password, which could be used to connect to Wi-Fi or perform a dictionary attack.
CVE-2019-17504	11/10/2019	11/10/2019	An issue was discovered in Kirona Dynamic Resource Scheduling (DRS) 5.5.3.5. A reflected Cross-site scripting (XSS) vulnerability allows remote attackers to inject arbitrary web script via the /osm/report/ password parameter.

CVE ID	Publish Date	Update Date	Description
CVE-2019-17503	11/10/2019	11/10/2019	An issue was discovered in Kirona Dynamic Resource Scheduling (DRS) 5.5.3.5. An unauthenticated user can access /osm/REGISTER.cmd (aka /osm_tiles/REGISTER.cmd) directly: it contains sensitive information about the database through the SQL queries within this batch file. This file exposes SQL database information such as database version, table name, column name, etc.
CVE-2019-17502	12/10/2019	12/10/2019	Hydra through 0.1.8 has a NULL pointer dereference and daemon crash when processing POST requests that lack a Content-Length header. read.c, request.c, and util.c contribute to this. The process_header_end() function calls boa_atoi(), which ultimately calls atoi() on a NULL pointer.
CVE-2019-17499	11/10/2019	11/10/2019	The setter.xml component of the Common Gateway Interface on Compal CH7465LG 6.12.18.25-2p4 devices does not properly validate ping command arguments, which allows remote authenticated users to execute OS commands as root via shell metacharacters in the Target_IP parameter.
CVE-2019-17497	10/10/2019	10/10/2019	Tracker PDF-XChange Editor before 8.0.330.0 has an NTLM SSO hash theft vulnerability using crafted FDF or XFDF files (a related issue to CVE-2018-4993). For example, an NTLM hash is sent for a link to \\192.168.0.2\C$\file.pdf without user interaction.
CVE-2019-17496	10/10/2019	10/10/2019	Craft CMS before 3.3.8 has stored XSS via a name field. This field is mishandled during site deletion.
CVE-2019-17495	10/10/2019	11/10/2019	A Cascading Style Sheets (CSS) injection vulnerability in Swagger UI before 3.23.11 allows attackers to use the Relative Path Overwrite (RPO) technique to perform CSS-based input field value exfiltration, such as exfiltration of a CSRF token value. In other words, this product intentionally allows the embedding of untrusted JSON data from remote servers, but it was not previously known that <style>@import within the JSON data was a functional attack method.
CVE-2019-17494	10/10/2019	11/10/2019	laravel-bjyblog 6.1.1 has XSS via a crafted URL.

CVE ID	Publish Date	Update Date	Description
CVE-2019-17493	10/10/2019	11/10/2019	Jiangnan Online Judge (aka jnoj) 0.8.0 has XSS via the Problem[sample_input] parameter to web/admin/problem/create or web/polygon/problem/update.
CVE-2019-17491	10/10/2019	11/10/2019	Jiangnan Online Judge (aka jnoj) 0.8.0 has XSS via the Problem[description] parameter to web/admin/problem/create or web/polygon/problem/update.
CVE-2019-17490	10/10/2019	11/10/2019	app\modules\polygon\controllers\ProblemController in Jiangnan Online Judge (aka jnoj) 0.8.0 allows arbitrary file upload, as demonstrated by PHP code (with a .php filename but the image/png content type) to the web/polygon/problem/tests URI.
CVE-2019-17489	10/10/2019	11/10/2019	Jiangnan Online Judge (aka jnoj) 0.8.0 has XSS via the Problem[title] parameter to web/polygon/problem/create or web/polygon/problem/update or web/admin/problem/create.
CVE-2019-17488	10/10/2019	11/10/2019	b3log Symphony (aka Sym) before 3.6.0 has XSS via the HTTP User-Agent header.
CVE-2019-17455	10/10/2019	10/10/2019	Libntlm through 1.5 relies on a fixed buffer size for tSmbNtlmAuthRequest, tSmbNtlmAuthChallenge, and tSmbNtlmAuthResponse read and write operations, as demonstrated by a stack-based buffer over-read in buildSmbNtlmAuthRequest in smbutil.c for a crafted NTLM request.
CVE-2019-17454	10/10/2019	11/10/2019	Bento4 1.5.1.0 has a NULL pointer dereference in AP4_Descriptor::GetTag in Core/Ap4Descriptor.h, related to AP4_StsdAtom::GetSampleDescription in Core/Ap4StsdAtom.cpp, as demonstrated by mp4info.
CVE-2019-17453	10/10/2019	11/10/2019	Bento4 1.5.1.0 has a NULL pointer dereference in AP4_DescriptorListWriter::Action in Core/Ap4Descriptor.h, related to AP4_IodsAtom::WriteFields in Core/Ap4IodsAtom.cpp, as demonstrated by mp4encrypt or mp4compact.
CVE-2019-17452	10/10/2019	11/10/2019	Bento4 1.5.1.0 has a NULL pointer dereference in AP4_DescriptorListInspector::Action in Core/Ap4Descriptor.h, related to AP4_IodsAtom::InspectFields in Core/Ap4IodsAtom.cpp, as demonstrated by mp4dump.

CVE ID	Publish Date	Update Date	Description
CVE-2019-17451	10/10/2019	10/10/2019	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32. It is an integer overflow leading to a SEGV in _bfd_dwarf2_find_nearest_line in dwarf2.c, as demonstrated by nm.
CVE-2019-17450	10/10/2019	10/10/2019	find_abstract_instance in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32, allows remote attackers to cause a denial of service (infinite recursion and application crash) via a crafted ELF file.
CVE-2019-17449	10/10/2019	10/10/2019	Avira Software Updater before 2.0.6.21094 allows a DLL side-loading attack.
CVE-2019-17434	10/10/2019	10/10/2019	LavaLite through 5.7 has XSS via a crafted account name that is mishandled on the Manage Clients screen.
CVE-2019-17433	10/10/2019	10/10/2019	z-song laravel-admin 1.7.3 has XSS via the Slug or Name on the Roles screen, because of mishandling on the "Operation log" screen.
CVE-2019-17432	10/10/2019	10/10/2019	An issue was discovered in fastadmin 1.0.0.20190705_beta. There is a public/admin/general.config/edit CSRF vulnerability, as demonstrated by resultant XSS via the row[name] parameter.
CVE-2019-17431	10/10/2019	11/10/2019	An issue was discovered in fastadmin 1.0.0.20190705_beta. There is a public/index.php/admin/auth/admin/add CSRF vulnerability.
CVE-2019-17430	10/10/2019	10/10/2019	EyouCms through 2019-07-11 has XSS related to the login.php web_recordnum parameter.
CVE-2019-17429	10/10/2019	10/10/2019	Adhouma CMS through 2019-10-09 has SQL Injection via the post.php p_id parameter.
CVE-2019-17427	9/10/2019	11/10/2019	In Redmine before 3.4.11 and 4.0.x before 4.0.4, persistent XSS exists due to textile formatting errors.

CVE ID	Publish Date	Update Date	Description
CVE-2019-17426	9/10/2019	10/10/2019	Automattic Mongoose through 5.7.4 allows attackers to bypass access control (in some applications) because any query object with a _bsontype attribute is ignored. For example, adding "_bsontype":"a" can sometimes interfere with a query filter. NOTE: this CVE is about Mongoose's failure to work around this _bsontype special case that exists in older versions of the bson parser (aka the mongodb/js-bson project).
CVE-2019-17420	9/10/2019	9/10/2019	In OISF LibHTP before 0.5.31, as used in Suricata 4.1.4 and other products, an HTTP protocol parsing error causes the http_-header signature to not alert on a response with a single \r\n ending.
CVE-2019-17419	9/10/2019	10/10/2019	An issue was discovered in MetInfo 7.0. There is SQL injection via the admin/?n=user&c=admin_user&a=doGetUserInfo id parameter.