Website reconnaissance report

OSINT Executive Summary

OSINT report is publicly available information on a website. From OSINT we will be able to gain basic information such as operating system, IP address, web frameworks, and sub-domains of the target website. We can also search for open ports and vulnerabilities in the target and its subdomains. This report presents the results of the reconnaissance activities conducted on the website “certifiedhacker.com”. There are lots of free online services available to gather information on the website and we are gonna use some of the known and reliable sources for the report. Tools and frameworks used for reconnaissance will be mentioned below.

Tools used

- Whois lookup
- Nslookup
- Netcraft
- DNS recon
- Wafw00f
- Dnsdumpster
- Whatweb
- Google dorks
- Knockpy
- Shodan.io
- Nmap
- Dns map
- Spiderfoot

Infrastructure Footprinting

An IP address is an essential part of gathering information on a website. It is necessary to classify sub-domains further and to perform active reconnaissance. IP addresses can be found for a website using tools such as Whois lookup, NS lookup, and DNS recon.

Whois Lookup

Whois lookup can be accessed from the command line by simply typing whois followed by the domain name. We can also use the Whois.com website which would provide the graphical user interface to interpret the data.

Cmd: Whois certifiedhacker.com

You can also use the Whois.com website for a graphical interface in which you just need to enter the domain name that you want to gather information about.

Whois Record for CertifiedHacker.com

− Domain Profile

Registrar	Network Solutions, LLC IANA ID: 2 URL: http://networksolutions.com Whois Server: whois.networksolutions.com domain.operations@web.com (p) +1.8777228662
Registrar Status	clientTransferProhibited
Dates	7,739 days old Created on 2002-07-30 Expires on 2024-07-29 Updated on 2023-08-22
Name Servers	NS1.BLUEHOST.COM (has 2,485,535 domains) NS2.BLUEHOST.COM (has 2,485,535 domains)
IP Address	162.241.216.11 - 1,441 other sites hosted on this server
IP Location	- Utah - Provo - Unified Layer
ASN	AS46606 UNIFIEDLAYER-AS-1, US (registered Oct 24, 2008)
Domain Status	Registered And No Website
IP History	13 changes on 13 unique IP addresses over 17 years
Registrar History	3 registrars with 3 drops
Hosting History	6 changes on 4 unique name servers over 20 years

```
Domain Name: CERTIFIEDHACKER.COM
Registry Domain ID: 88849376_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2023-08-22T07:58:34Z
Creation Date: 2002-07-30T00:32:00Z
Registrar Registration Expiration Date: 2024-07-29T04:00:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibite
d
Registry Registrant ID:
Registrant Name: PERFECT PRIVACY, LLC
Registrant Organization:
Registrant Street: 5335 Gate Parkway care of Network Solutions PO Box 459
Registrant City: Jacksonville
Registrant State/Province: FL
Registrant Postal Code: 32256
Registrant Country: US
Registrant Phone: +1.5707088622
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: kq9t994x73e@networksolutionsprivateregistration.com
Registry Admin ID:
Admin Name: PERFECT PRIVACY, LLC
Admin Organization:
Admin Street: 5335 Gate Parkway care of Network Solutions PO Box 459
Admin City: Jacksonville
Admin State/Province: FL
Admin Postal Code: 32256
Admin Country: US
Admin Phone: +1.5707088622
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: kq9t994x73e@networksolutionsprivateregistration.com
```

```
Registry Tech ID:
Tech Name: PERFECT PRIVACY, LLC
Tech Organization:
Tech Street: 5335 Gate Parkway care of Network Solutions PO Box 459
Tech City: Jacksonville
Tech State/Province: FL
Tech Postal Code: 32256
Tech Country: US
Tech Phone: +1.5707088622
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: kq9t994x73e@networksolutionsprivateregistration.com
Name Server: NS1.BLUEHOST.COM
Name Server: NS2.BLUEHOST.COM
DNSSEC: unsigned
Registrar Abuse Contact Email: domain.operations@web.com
Registrar Abuse Contact Phone: +1.8777228662
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

https://www.icann.org/resources/pages/epp-status-codes-2014-06-16-en.
```

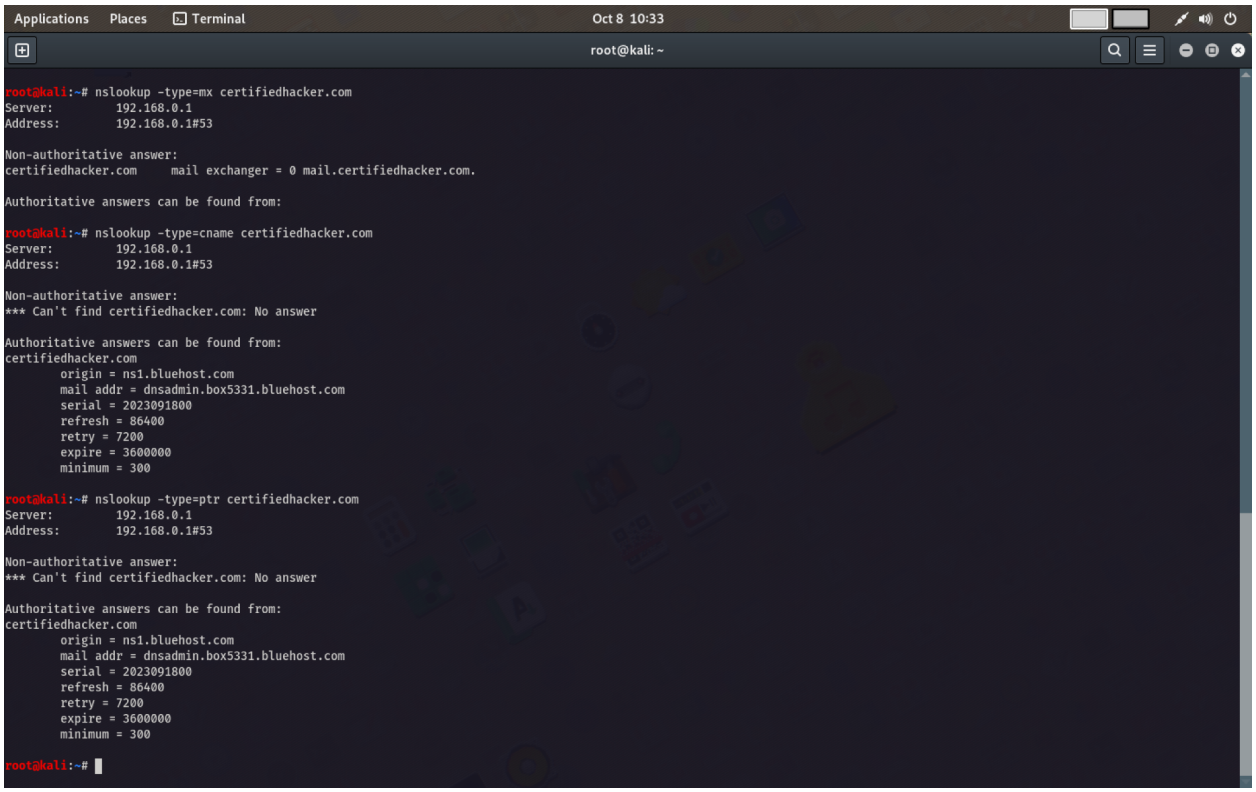
NSlookup

NSlookup will give domain information and IP address hostname for a specific domain. You can ask for a specific information by specifying the type of record you are searching for and the command for that as follows

Nslookup type=ns certifiedhacker.com

You can also specify
A : IPv4 address
AAAA : IPv6 address
CNAME : Information about the domain's alternate name
LOC : specifies the geographic location of a domain
PTR : maps IP addresses to a hostname and is also responsible for mail exchange
MX : Responsible for mail exchange. MX records map domain name to mail servers

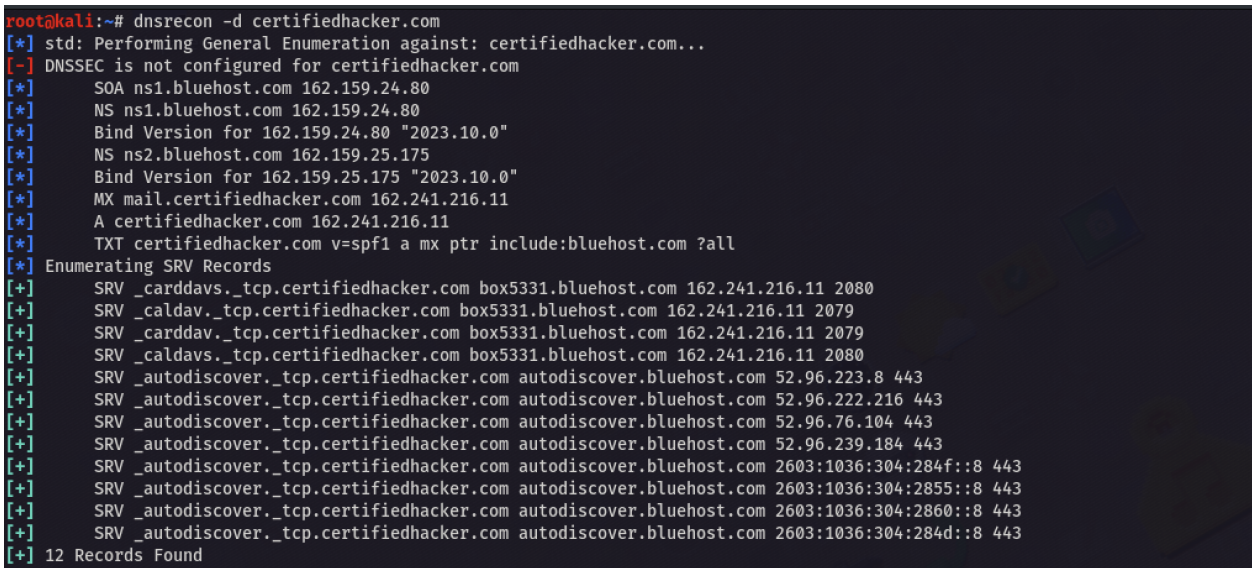
```
root@kali:~# nslookup -type=a certifiedhacker.com
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
Name:   certifiedhacker.com
Address: 162.241.216.11

root@kali:~# nslookup -type=aaaa certifiedhacker.com
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
*** Can't find certifiedhacker.com: No answer
```



DNS Recon

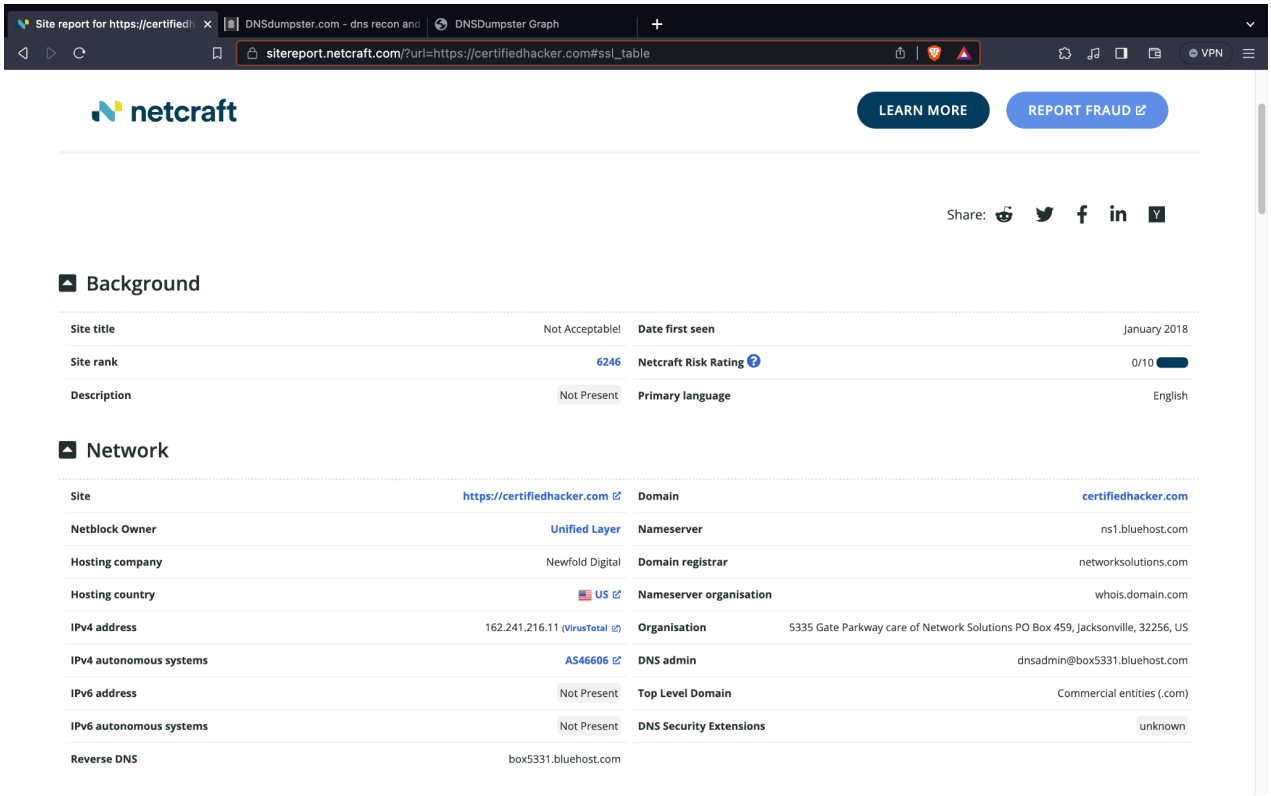
DNS recon is a Python script to perform DNS reconnaissance, enumeration, and information gathering.

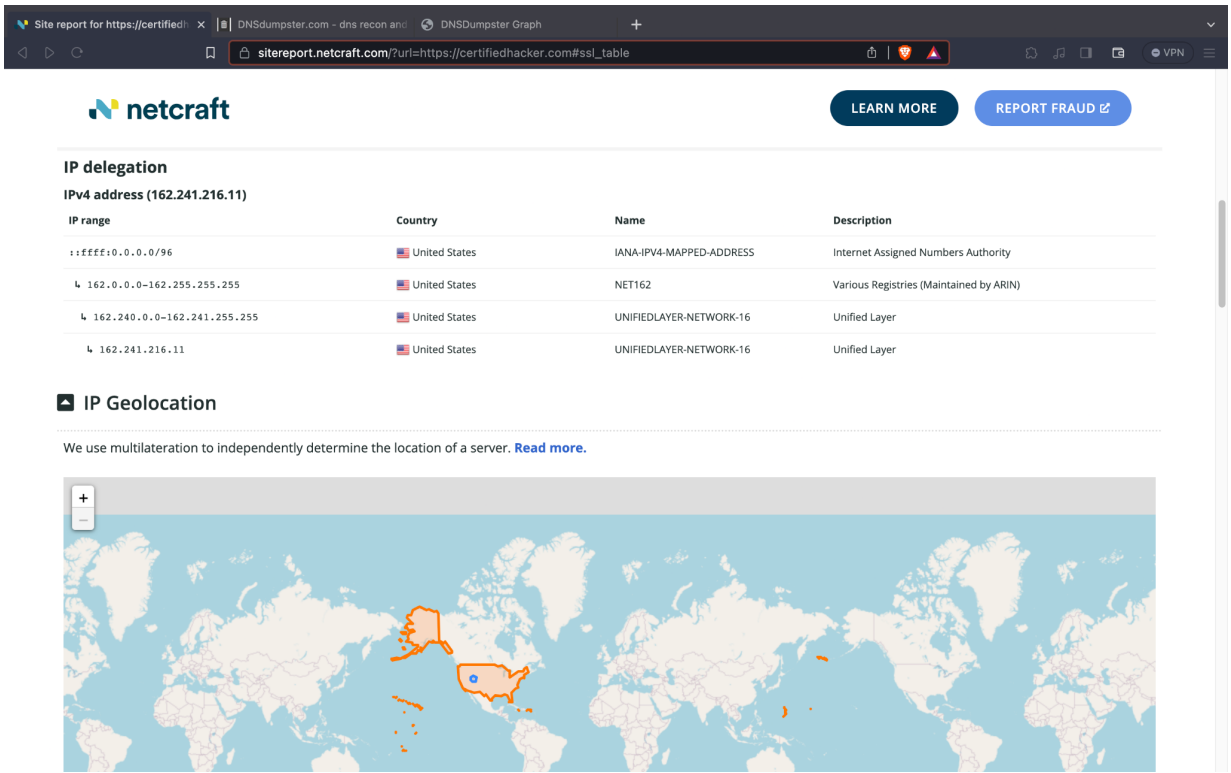
Dnsrecon <options> <domain name>

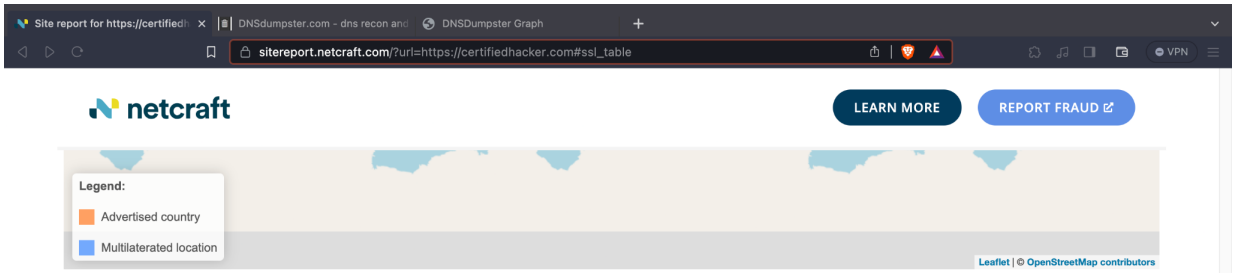


Netcraft

Netcraft is a powerful reconnaissance tool that helps gather information about a domain including SSL/TLS information, IP geolocation, Hosting history, and much more. Netcraft is an easy-to-use tool as you have to enter only the website you want to gather information about. We can use netcraft to identify what a website is running and enumerate information about that particular site.

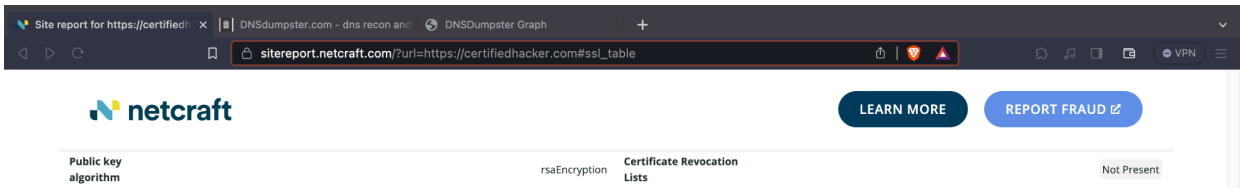

Site report for https://certifiedh
DNSdumpster.com - dns recon and
DNSDumpster Graph
sitereport.netcraft.com/?url=https://certifiedhacker.com#ssl_table
VPN
netcraft
LEARN MORE
REPORT FRAUD
Share:
Background
Site title
Not Acceptable!
Date first seen
January 2018
Site rank
6246
Netcraft Risk Rating
0/10
Description
Not Present
Primary language
English
Network
Site
https://certifiedhacker.com
Domain
certifiedhacker.com
Netblock Owner
Unified Layer
Nameserver
ns1.bluehost.com
Hosting company
Newfold Digital
Domain registrar
networksolutions.com
Hosting country
US
Nameserver organisation
whois.domain.com
IPv4 address
162.241.216.11 (VirusTotal)
Organisation
5335 Gate Parkway care of Network Solutions PO Box 459, Jacksonville, 32256, US
IPv4 autonomous systems
AS46606
DNS admin
dnsadmin@box5331.bluehost.com
IPv6 address
Not Present
Top Level Domain
Commercial entities (.com)
IPv6 autonomous systems
Not Present
DNS Security Extensions
unknown
Reverse DNS
box5331.bluehost.com


Site report for https://certifiedh
DNSdumpster.com - dns recon and
DNSDumpster Graph
sitereport.netcraft.com/?url=https://certifiedhacker.com#ssl_table
VPN
netcraft
LEARN MORE
REPORT FRAUD
IP delegation
IPv4 address (162.241.216.11)
IP range
Country
Name
Description
::ffff:0.0.0.0/96
United States
IANA-IPV4-MAPPED-ADDRESS
Internet Assigned Numbers Authority
↳ 162.0.0.0-162.255.255.255
United States
NET162
Various Registries (Maintained by ARIN)
↳ 162.240.0.0-162.241.255.255
United States
UNIFIEDLAYER-NETWORK-16
Unified Layer
↳ 162.241.216.11
United States
UNIFIEDLAYER-NETWORK-16
Unified Layer
IP Geolocation
We use multilateration to independently determine the location of a server. Read more.



SSL/TLS

Assurance	Domain validation	**Perfect Forward Secrecy**	Yes
Common name	www.certifiedhacker.com	**Supported TLS Extensions**	RFC8446 supported versions, RFC8446 key share, RFC4366 server name, RFC7301 application-layer protocol negotiation
Organisation	Not Present	**Application-Layer Protocol Negotiation**	h2
State	Not Present	**Next Protocol Negotiation**	Not Present
Country	Not Present	**Issuing organisation**	Let's Encrypt
Organisational unit	Not Present	**Issuer common name**	R3
Subject Alternative Name	autodiscover.certifiedhacker.com, certifiedhacker.com, cpanel.certifiedhacker.com, cpcalendars.certifiedhacker.com, cpcontacts.certifiedhacker.com, mail.certifiedhacker.com, webdisk.certifiedhacker.com, webmail.certifiedhacker.com, www.certifiedhacker.com	**Issuer unit**	Not Present
Validity period	From Aug 22 2023 to Nov 20 2023 (2 months, 4 weeks)	**Issuer location**	Not Present
Matches hostname	Yes	**Issuer country**	US
Server	Apache	**Issuer state**	Not Present



Public key algorithm	rsaEncryption	**Certificate Revocation Lists**	Not Present
Protocol version	TLSv1.3	**Certificate Hash**	LSgjDNmnllzWi3GqU8wreyYWSw0
Public key length	2048	**Public Key Hash**	77bf1d58f368b6485fe23accba58000c4e594b4bd1af1c427d18fcd3703add18
Certificate check	ok	**OCSP servers**	http://r3.o.lencr.org - *100% uptime in the past 24 hours* Performance Graph
Signature algorithm	sha256WithRSAEncryption	**OCSP stapling response**	No response received
Serial number	0x04ad5869d33a6a195bbf6d19d87974049e13		
Cipher	TLS_AES_256_GCM_SHA384		
Version number	0x02		

Certificate Transparency

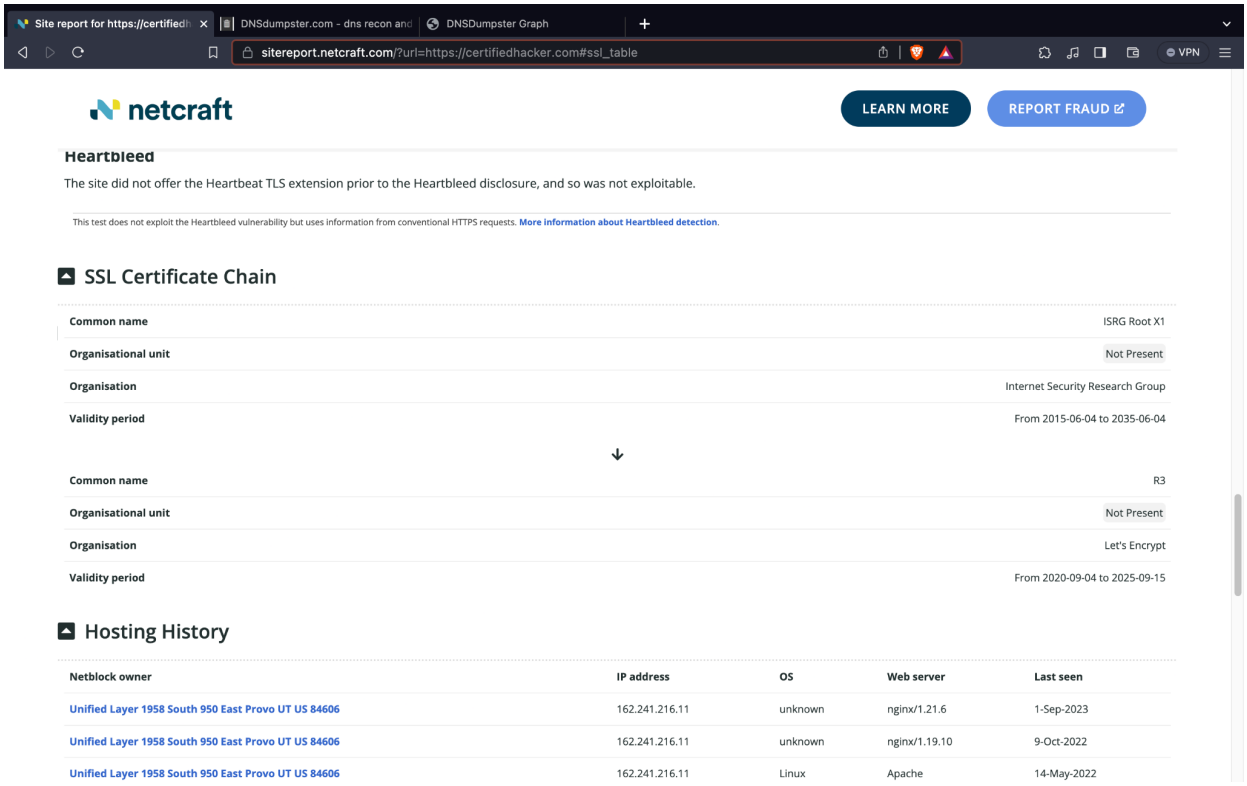
Signed Certificate Timestamps (SCTs)

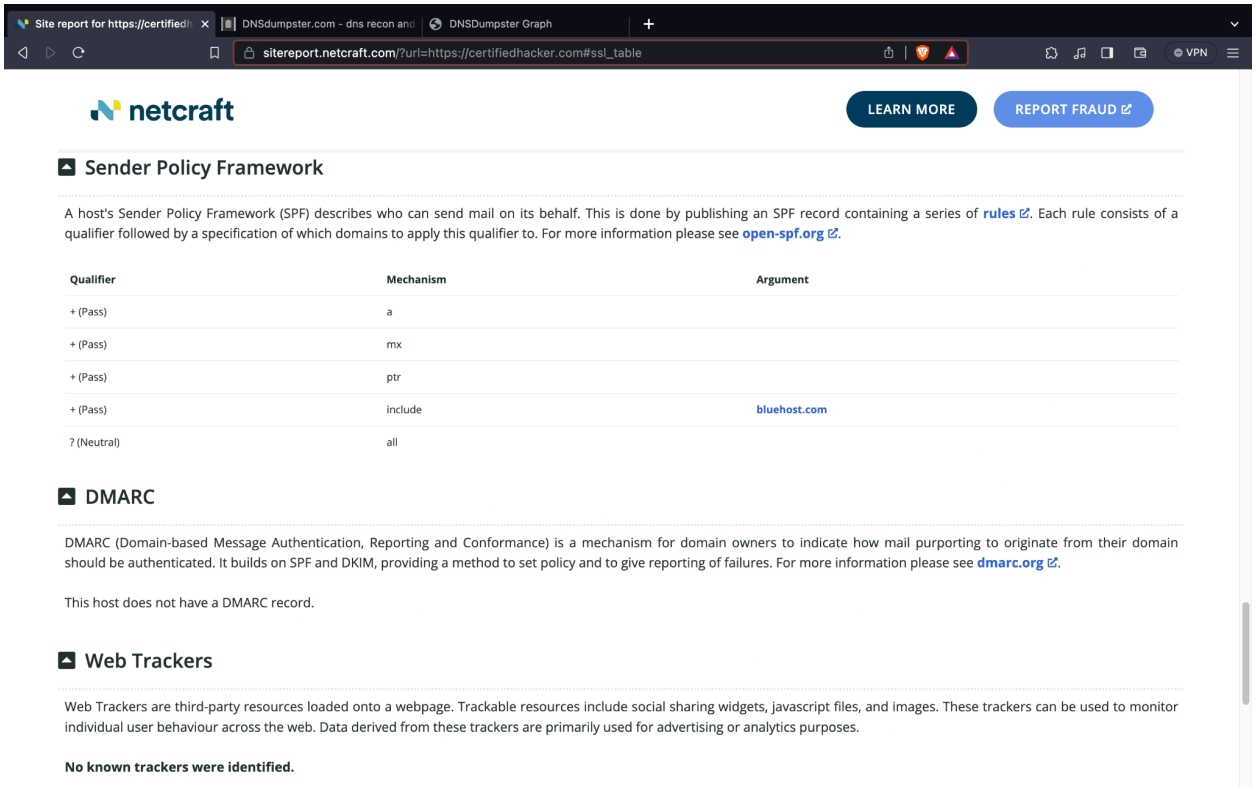
Source	Log	Timestamp	Signature Verification
Certificate	Let's Encrypt Oak 2023 `tz77JN+cTbp18jnFulj0bF38Qs96nzXEnh0JgSXttJk=`	2023-08-22 16:01:59	Success
Certificate	Google Xenon 2023 `rfe++nz/EMiLnT2cHj4YarRnKV3PsQwkyoWGNOvcgoo=`	2023-08-22 16:01:59	Success

SSLv3/POODLE

This site does not support the SSL version 3 protocol.

More information about SSL version 3 and the POODLE vulnerability.

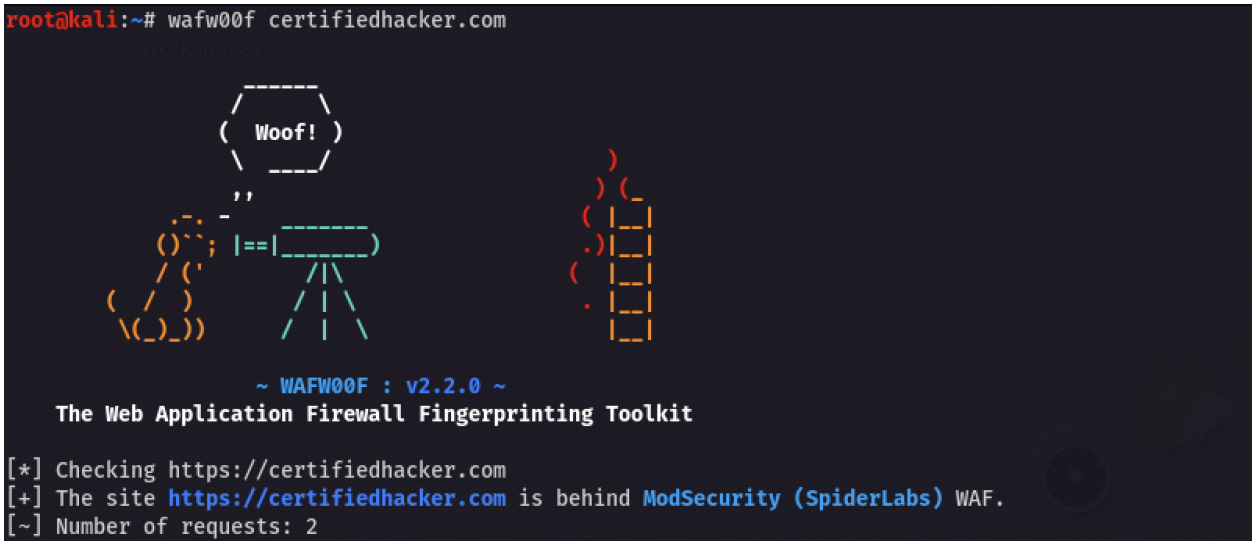

Site report for https://certifiedh
DNSdumpster.com - dns recon and
DNSDumpster Graph
sitereport.netcraft.com/?url=https://certifiedhacker.com#ssl_table
VPN
netcraft
LEARN MORE
REPORT FRAUD
Heartbleed
The site did not offer the Heartbeat TLS extension prior to the Heartbleed disclosure, and so was not exploitable.
This test does not exploit the Heartbleed vulnerability but uses information from conventional HTTPS requests. More information about Heartbleed detection.
SSL Certificate Chain
Common name ISRG Root X1
Organisational unit Not Present
Organisation Internet Security Research Group
Validity period From 2015-06-04 to 2035-06-04
Common name R3
Organisational unit Not Present
Organisation Let's Encrypt
Validity period From 2020-09-04 to 2025-09-15
Hosting History
Netblock owner | IP address | OS | Web server | Last seen
Unified Layer 1958 South 950 East Provo UT US 84606 | 162.241.216.11 | unknown | nginx/1.21.6 | 1-Sep-2023
Unified Layer 1958 South 950 East Provo UT US 84606 | 162.241.216.11 | unknown | nginx/1.19.10 | 9-Oct-2022
Unified Layer 1958 South 950 East Provo UT US 84606 | 162.241.216.11 | Linux | Apache | 14-May-2022


Site report for https://certifiedh
DNSdumpster.com - dns recon and
DNSDumpster Graph
sitereport.netcraft.com/?url=https://certifiedhacker.com#ssl_table
VPN
netcraft
LEARN MORE
REPORT FRAUD
Sender Policy Framework
A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of rules. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see open-spf.org.
Qualifier | Mechanism | Argument
+ (Pass) | a
+ (Pass) | mx
+ (Pass) | ptr
+ (Pass) | include | bluehost.com
? (Neutral) | all
DMARC
DMARC (Domain-based Message Authentication, Reporting and Conformance) is a mechanism for domain owners to indicate how mail purporting to originate from their domain should be authenticated. It builds on SPF and DKIM, providing a method to set policy and to give reporting of failures. For more information please see dmarc.org.
This host does not have a DMARC record.
Web Trackers
Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.
No known trackers were identified.

Wafw00f

Wafw00f is a firewall detection tool which helps identify the firewall provider and its type.

Cmd: wafw00f certifiedhacker.com

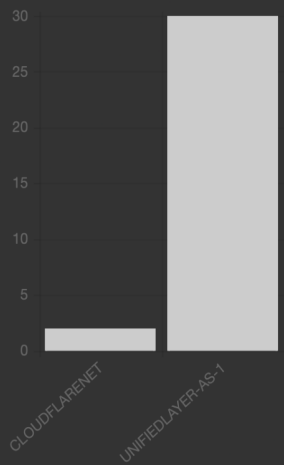


Dnsdumpster

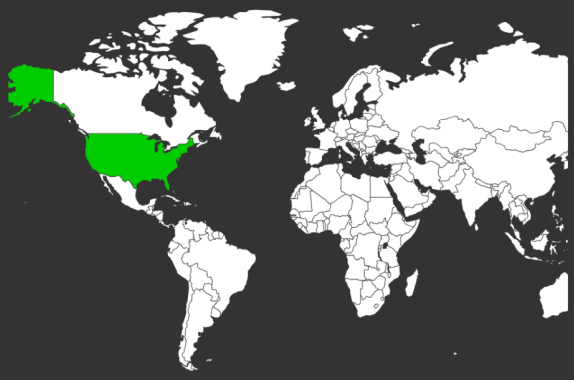
DNSdumpster.com is a FREE domain research tool that can discover hosts related to a domain. Finding visible hosts from the attackers perspective is an important part of the security assessment process. Its a web based reconnaissance tool so you just need to enter the domain you want to gather information on and no additional commands or keywords needed.

DNS Servers | MX Records | TXT Records | Host (A) Records | Domain Map

Hosting (IP block owners)



GeoIP of Host Locations



DNS Servers

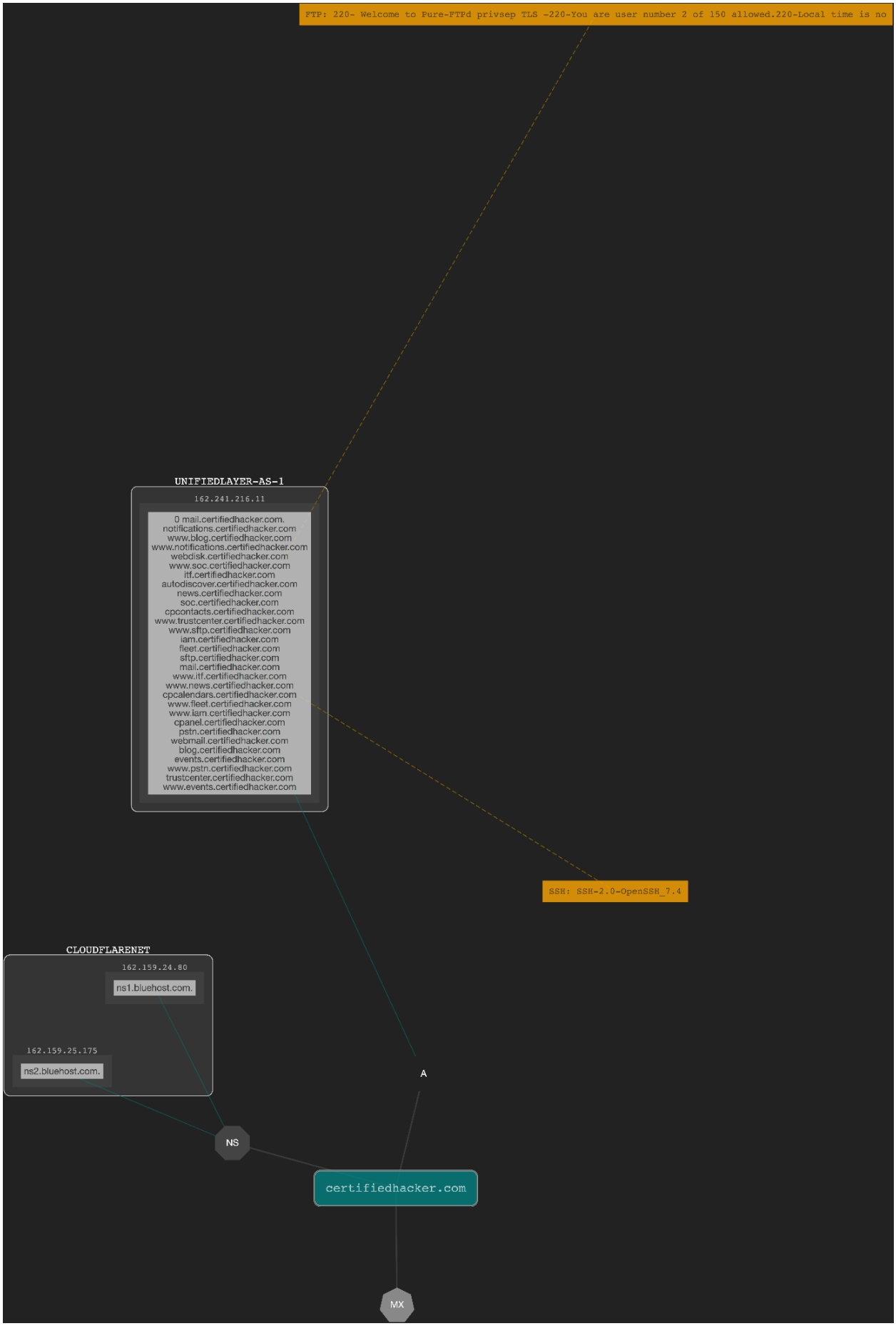
ns2.bluehost.com.	162.159.25.175 ns2.bluehost.com	CLOUDFLARENET unknown
ns1.bluehost.com.	162.159.24.80 ns1.bluehost.com	CLOUDFLARENET unknown

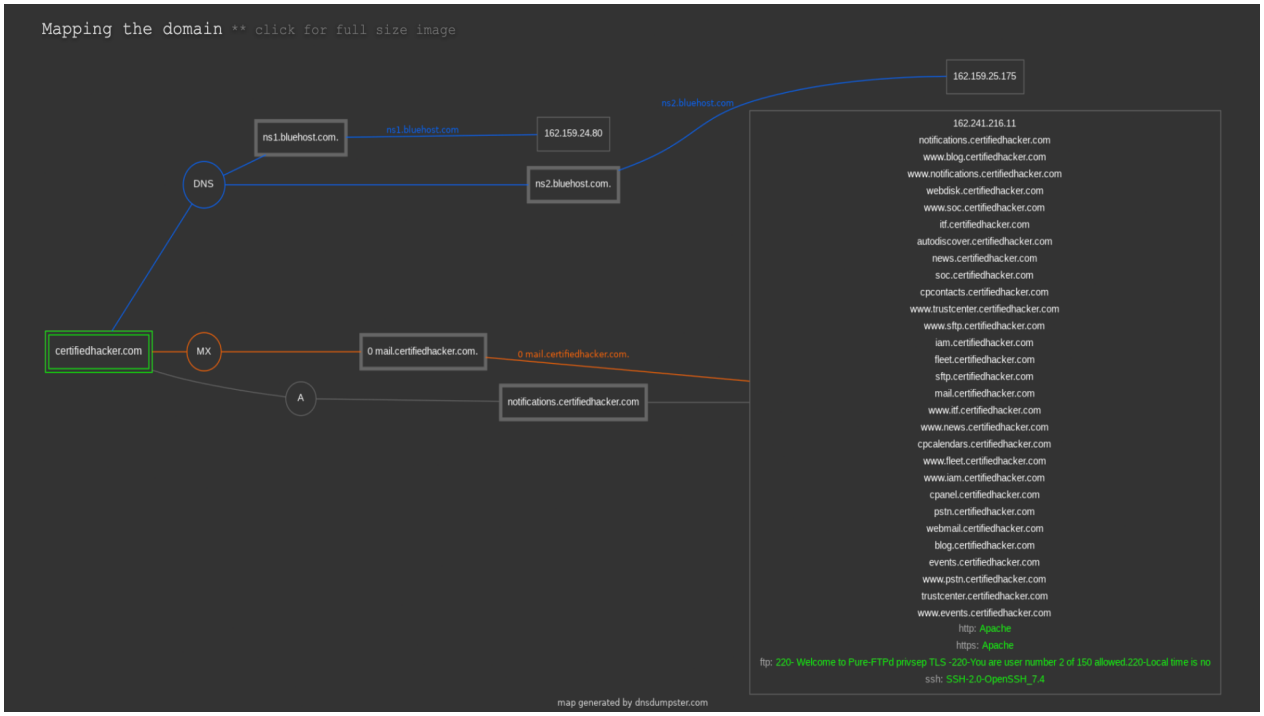
MX Records ** This is where email for the domain goes...

0 mail.certifiedhacker.com.	162.241.216.11 box5331.bluehost.com	UNIFIEDLAYER-AS-1 United States

TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

"v=spf1 a mx ptr include:bluehost.com ?all"


FTP: 220- Welcome to Pure-FTPd privsep TLS -220-You are user number 2 of 150 allowed.220-Local time is no
UNIFIEDLAYER-AS-1
162.241.216.11
0 mail.certifiedhacker.com.
notifications.certifiedhacker.com
www.blog.certifiedhacker.com
www.notifications.certifiedhacker.com
webdisk.certifiedhacker.com
www.soc.certifiedhacker.com
itf.certifiedhacker.com
autodiscover.certifiedhacker.com
news.certifiedhacker.com
soc.certifiedhacker.com
cpcontacts.certifiedhacker.com
www.trustcenter.certifiedhacker.com
www.sftp.certifiedhacker.com
iam.certifiedhacker.com
fleet.certifiedhacker.com
sftp.certifiedhacker.com
mail.certifiedhacker.com
www.itf.certifiedhacker.com
www.news.certifiedhacker.com
cpcalendars.certifiedhacker.com
www.fleet.certifiedhacker.com
www.iam.certifiedhacker.com
cpanel.certifiedhacker.com
pstn.certifiedhacker.com
webmail.certifiedhacker.com
blog.certifiedhacker.com
events.certifiedhacker.com
www.pstn.certifiedhacker.com
trustcenter.certifiedhacker.com
www.events.certifiedhacker.com
SSH: SSH-2.0-OpenSSH_7.4
CLOUDFLARENET
162.159.24.80
ns1.bluehost.com.
162.159.25.175
ns2.bluehost.com.
A
NS
certifiedhacker.com
MX

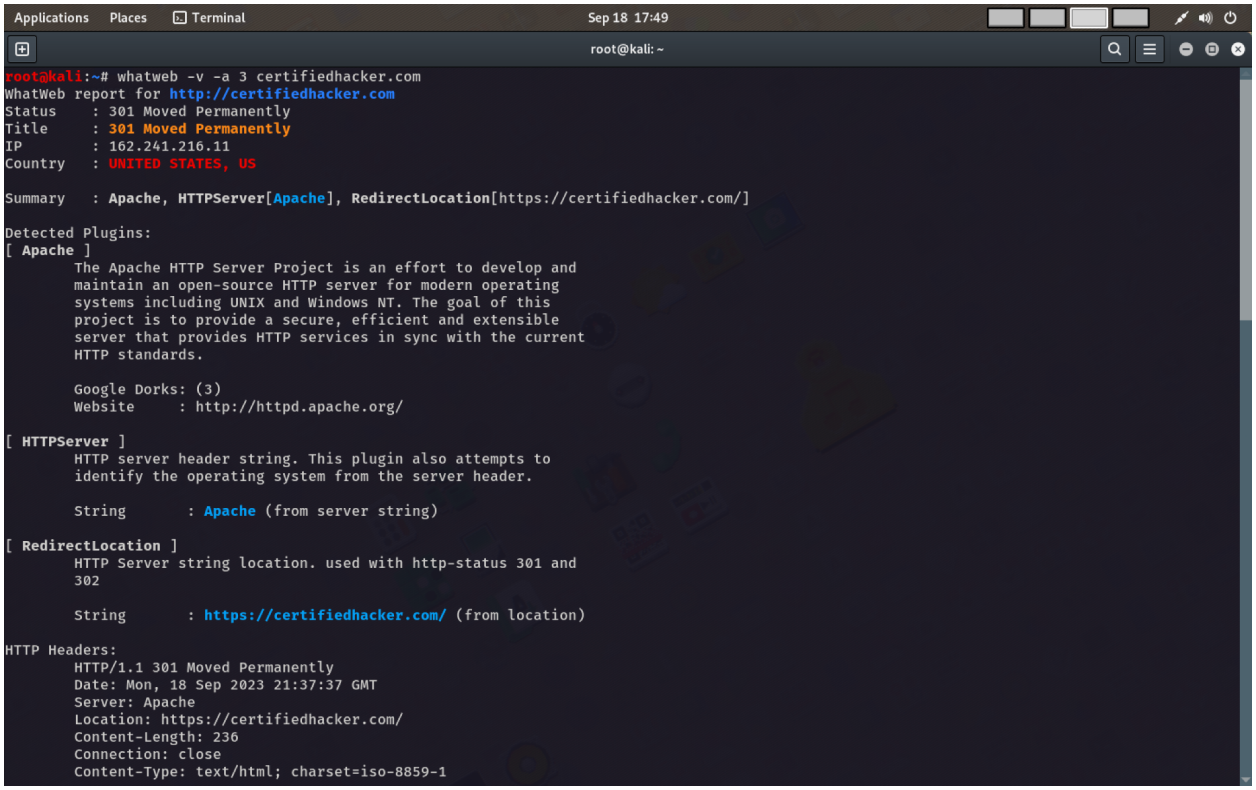


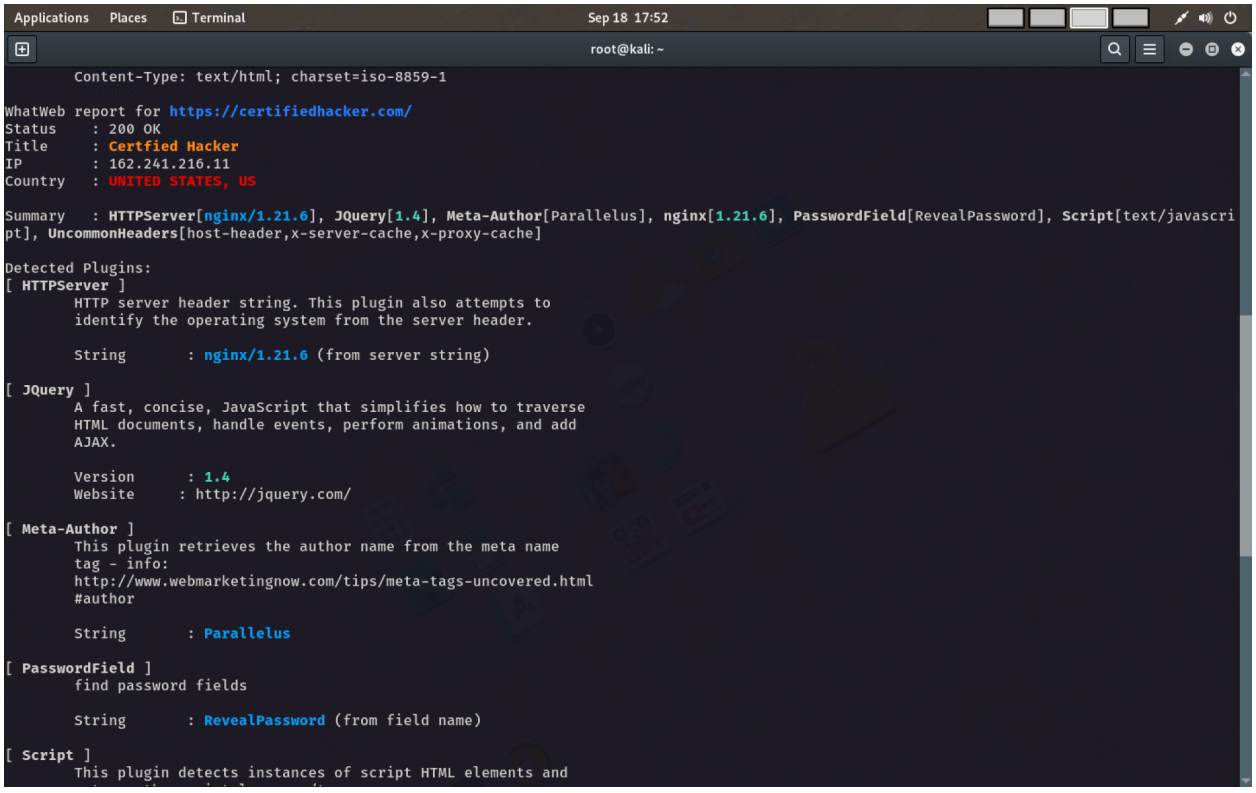
Whatweb

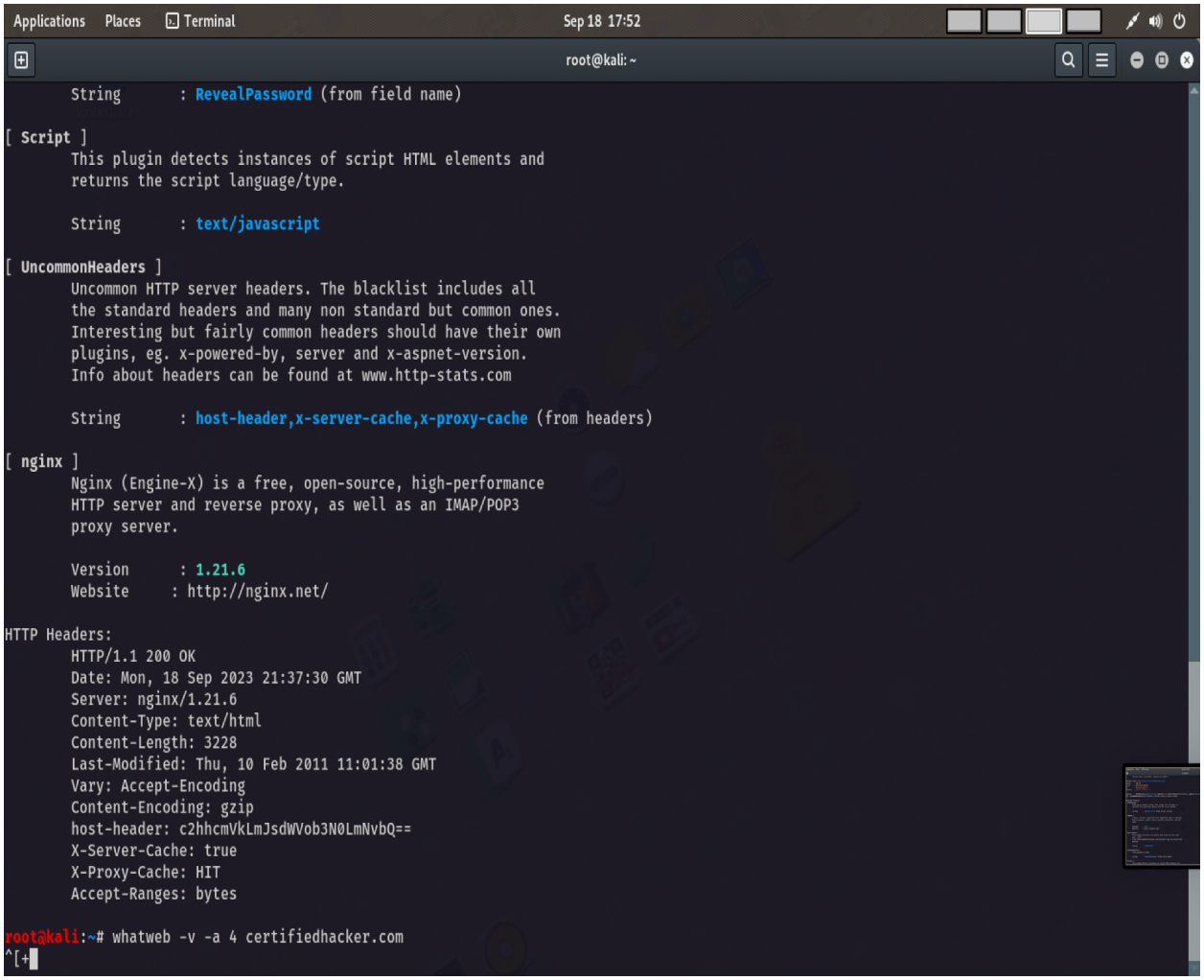
WhatWeb identifies websites. It recognizes web technologies including content management systems (CMS), blogging platforms, statistic/analytics packages, JavaScript libraries, web servers, and embedded devices.

Cmd: whatweb -v -a 3 <domain name>

-v : verbose
-a : sets the level of aggression
    1 - stealthy
    2 - aggressive
    3 - Heavy


Applications Places Terminal Sep 18 17:49
root@kali: ~
root@kali:~# whatweb -v -a 3 certifiedhacker.com
WhatWeb report for http://certifiedhacker.com
Status : 301 Moved Permanently
Title : 301 Moved Permanently
IP : 162.241.216.11
Country : UNITED STATES, US
Summary : Apache, HTTPServer[Apache], RedirectLocation[https://certifiedhacker.com/]
Detected Plugins:
[Apache]
The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows NT. The goal of this project is to provide a secure, efficient and extensible server that provides HTTP services in sync with the current HTTP standards.
Google Dorks: (3)
Website : http://httpd.apache.org/
[HTTPServer]
HTTP server header string. This plugin also attempts to identify the operating system from the server header.
String : Apache (from server string)
[RedirectLocation]
HTTP Server string location. used with http-status 301 and 302
String : https://certifiedhacker.com/ (from location)
HTTP Headers:
HTTP/1.1 301 Moved Permanently
Date: Mon, 18 Sep 2023 21:37:37 GMT
Server: Apache
Location: https://certifiedhacker.com/
Content-Length: 236
Connection: close
Content-Type: text/html; charset=iso-8859-1

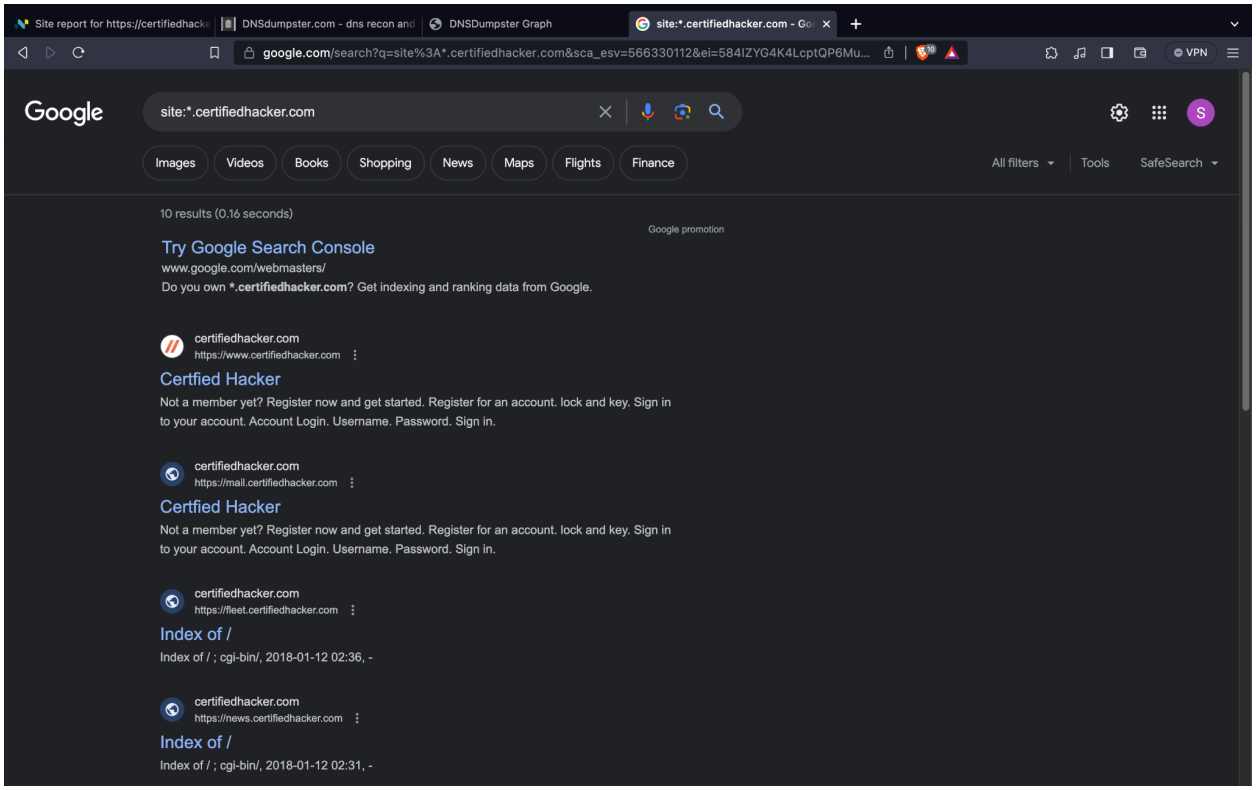

Applications Places Terminal Sep 18 17:52
root@kali: ~
Content-Type: text/html; charset=iso-8859-1
WhatWeb report for https://certifiedhacker.com/
Status : 200 OK
Title : Certfied Hacker
IP : 162.241.216.11
Country : UNITED STATES, US
Summary : HTTPServer[nginx/1.21.6], JQuery[1.4], Meta-Author[Parallelus], nginx[1.21.6], PasswordField[RevealPassword], Script[text/javascript], UncommonHeaders[host-header,x-server-cache,x-proxy-cache]
Detected Plugins:
[HTTPServer]
HTTP server header string. This plugin also attempts to identify the operating system from the server header.
String : nginx/1.21.6 (from server string)
[JQuery]
A fast, concise, JavaScript that simplifies how to traverse HTML documents, handle events, perform animations, and add AJAX.
Version : 1.4
Website : http://jquery.com/
[Meta-Author]
This plugin retrieves the author name from the meta name tag - info:
http://www.webmarketingnow.com/tips/meta-tags-uncovered.html
#author
String : Parallelus
[PasswordField]
find password fields
String : RevealPassword (from field name)
[Script]
This plugin detects instances of script HTML elements and

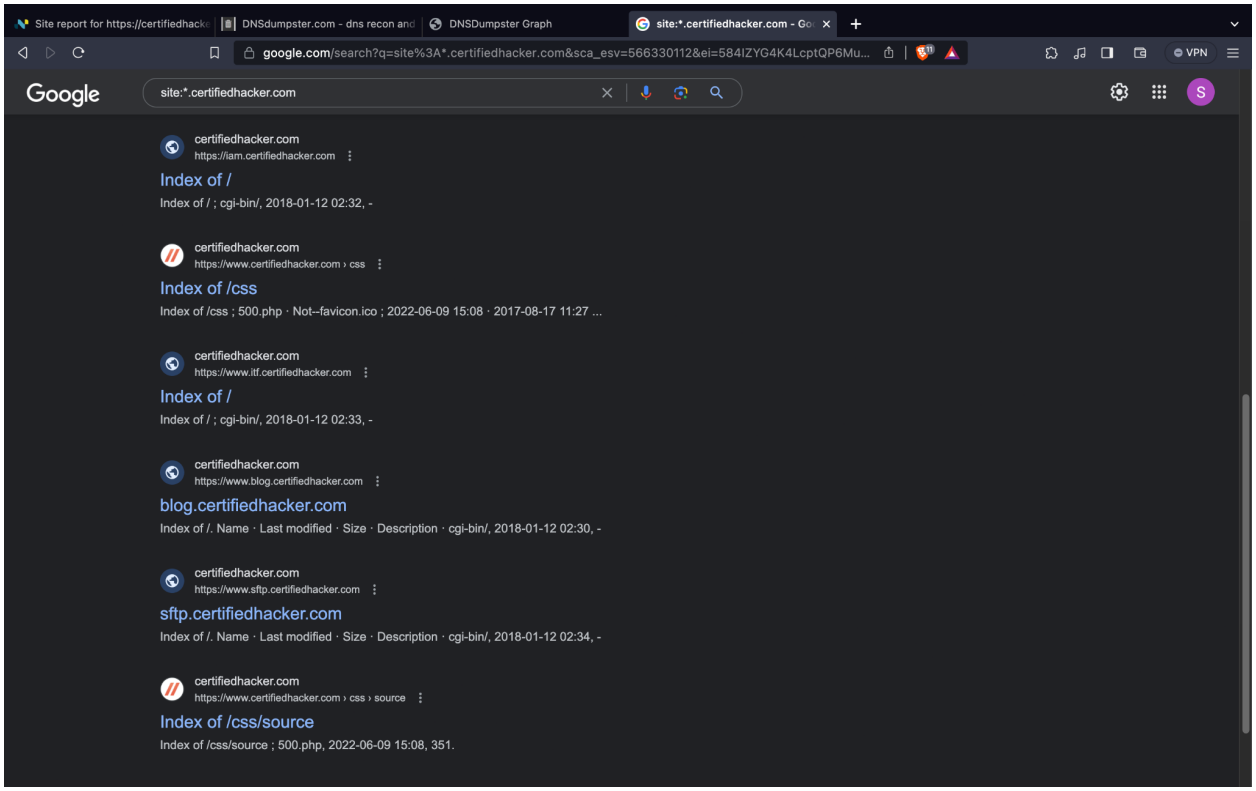


Google Dorks

Google Dorks is a search technique that uses advanced operators to search for information that is not typically indexed by search engines. To find the subdomains related to certifiedhacker.com you can simply use * infront of the domain name which will match any domain that is followed by the given domain name

Site: *.certifiedhacker.com

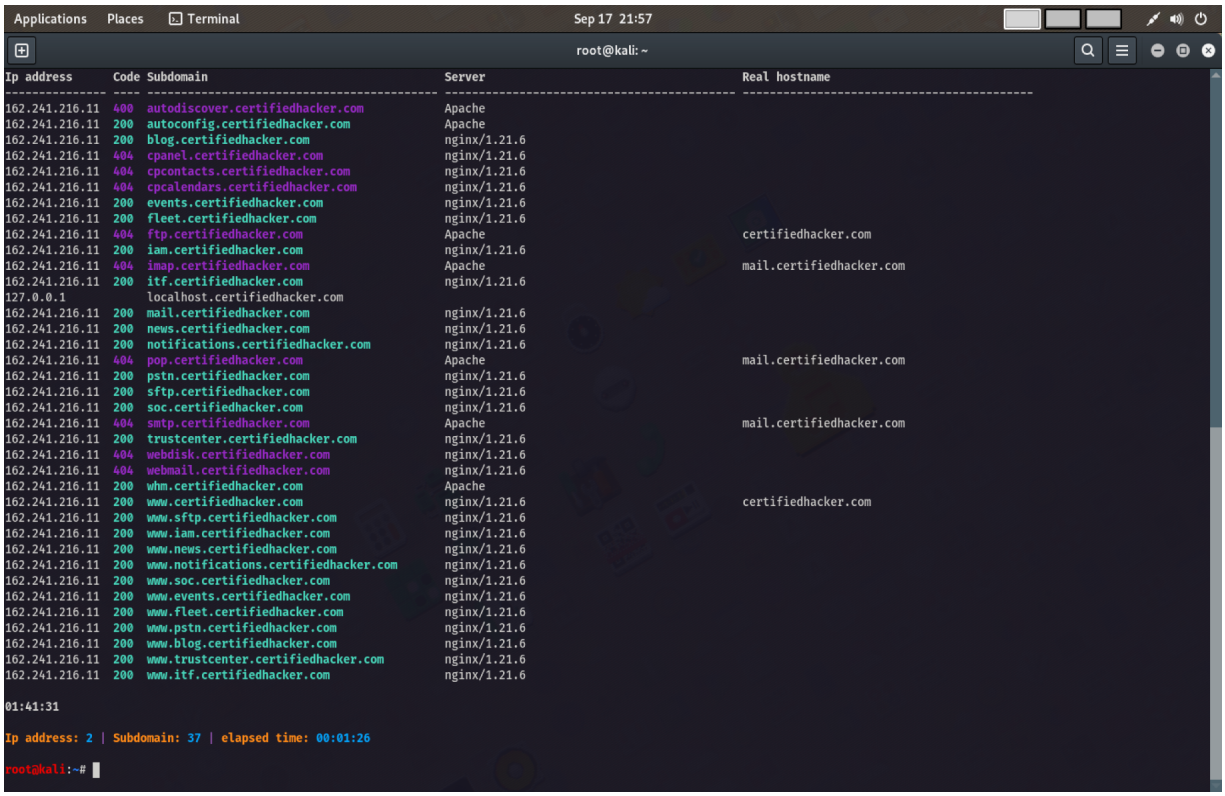

Site report for https://certifiedhacke
DNSdumpster.com - dns recon and
DNSDumpster Graph
site:*.certifiedhacker.com - Go
google.com/search?q=site%3A*.certifiedhacker.com&sca_esv=566330112&ei=584IZYG4K4LcptQP6Mu...
VPN
Google
site:*.certifiedhacker.com
Images
Videos
Books
Shopping
News
Maps
Flights
Finance
All filters
Tools
SafeSearch
10 results (0.16 seconds)
Google promotion
Try Google Search Console
www.google.com/webmasters/
Do you own *.certifiedhacker.com? Get indexing and ranking data from Google.
certifiedhacker.com
https://www.certifiedhacker.com
Certfied Hacker
Not a member yet? Register now and get started. Register for an account. lock and key. Sign in to your account. Account Login. Username. Password. Sign in.
certifiedhacker.com
https://mail.certifiedhacker.com
Certfied Hacker
Not a member yet? Register now and get started. Register for an account. lock and key. Sign in to your account. Account Login. Username. Password. Sign in.
certifiedhacker.com
https://fleet.certifiedhacker.com
Index of /
Index of / ; cgi-bin/, 2018-01-12 02:36, -
certifiedhacker.com
https://news.certifiedhacker.com
Index of /
Index of / ; cgi-bin/, 2018-01-12 02:31, -


Site report for https://certifiedhacke
DNSdumpster.com - dns recon and
DNSDumpster Graph
site:*.certifiedhacker.com - Go
google.com/search?q=site%3A*.certifiedhacker.com&sca_esv=566330112&ei=584IZYG4K4LcptQP6Mu...
VPN
Google
site:*.certifiedhacker.com
certifiedhacker.com
https://iam.certifiedhacker.com
Index of /
Index of / ; cgi-bin/, 2018-01-12 02:32, -
certifiedhacker.com
https://www.certifiedhacker.com › css
Index of /css
Index of /css ; 500.php · Not--favicon.ico ; 2022-06-09 15:08 · 2017-08-17 11:27 ...
certifiedhacker.com
https://www.itf.certifiedhacker.com
Index of /
Index of / ; cgi-bin/, 2018-01-12 02:33, -
certifiedhacker.com
https://www.blog.certifiedhacker.com
blog.certifiedhacker.com
Index of /. Name · Last modified · Size · Description · cgi-bin/, 2018-01-12 02:30, -
certifiedhacker.com
https://www.sftp.certifiedhacker.com
sftp.certifiedhacker.com
Index of /. Name · Last modified · Size · Description · cgi-bin/, 2018-01-12 02:34, -
certifiedhacker.com
https://www.certifiedhacker.com › css › source
Index of /css/source
Index of /css/source ; 500.php, 2022-06-09 15:08, 351.

Knockpy

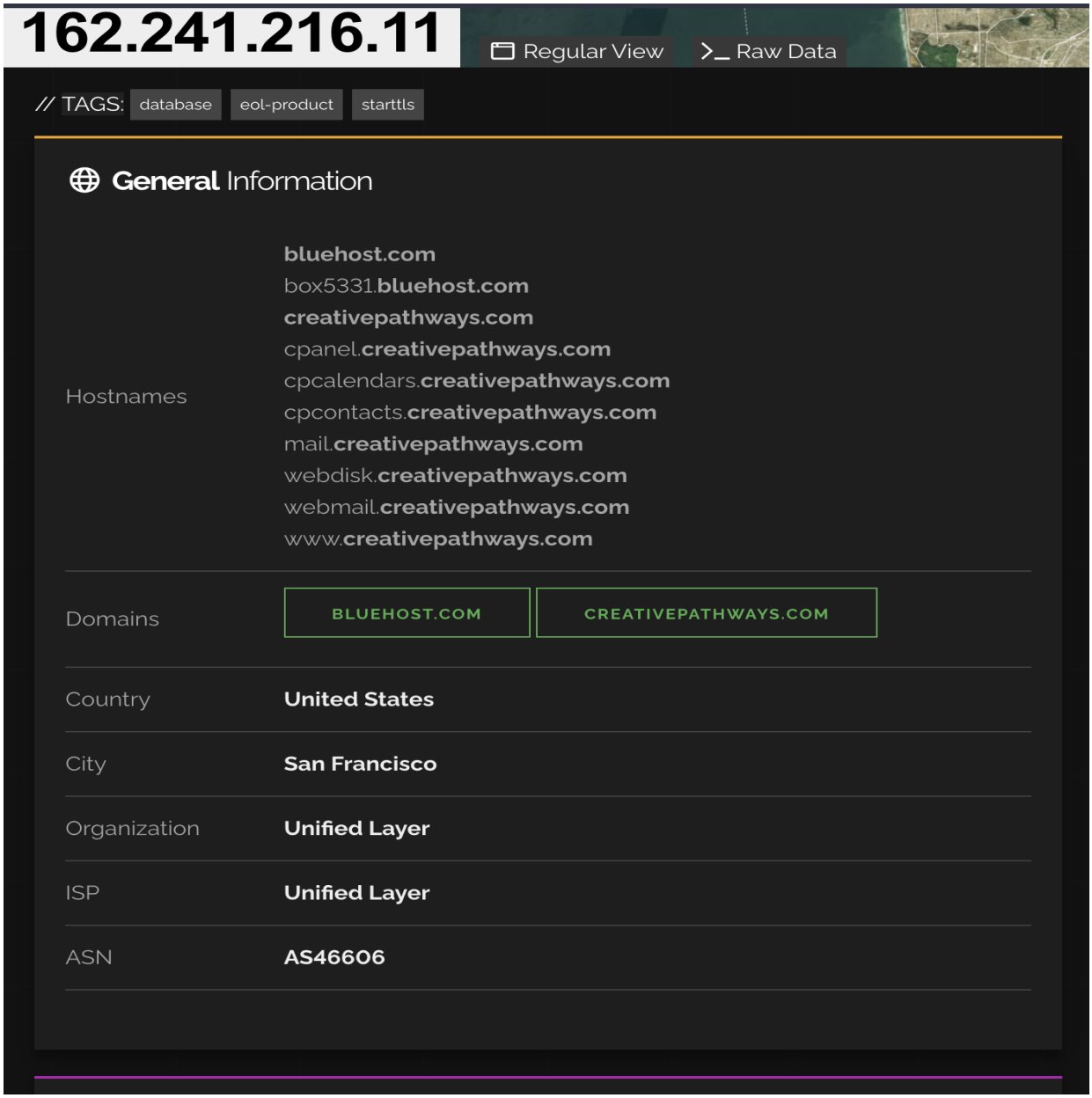
Knockpy is a portable and modular python3 tool designed to quickly enumerate subdomains on a target domain through passive reconnaissance and dictionary scan.

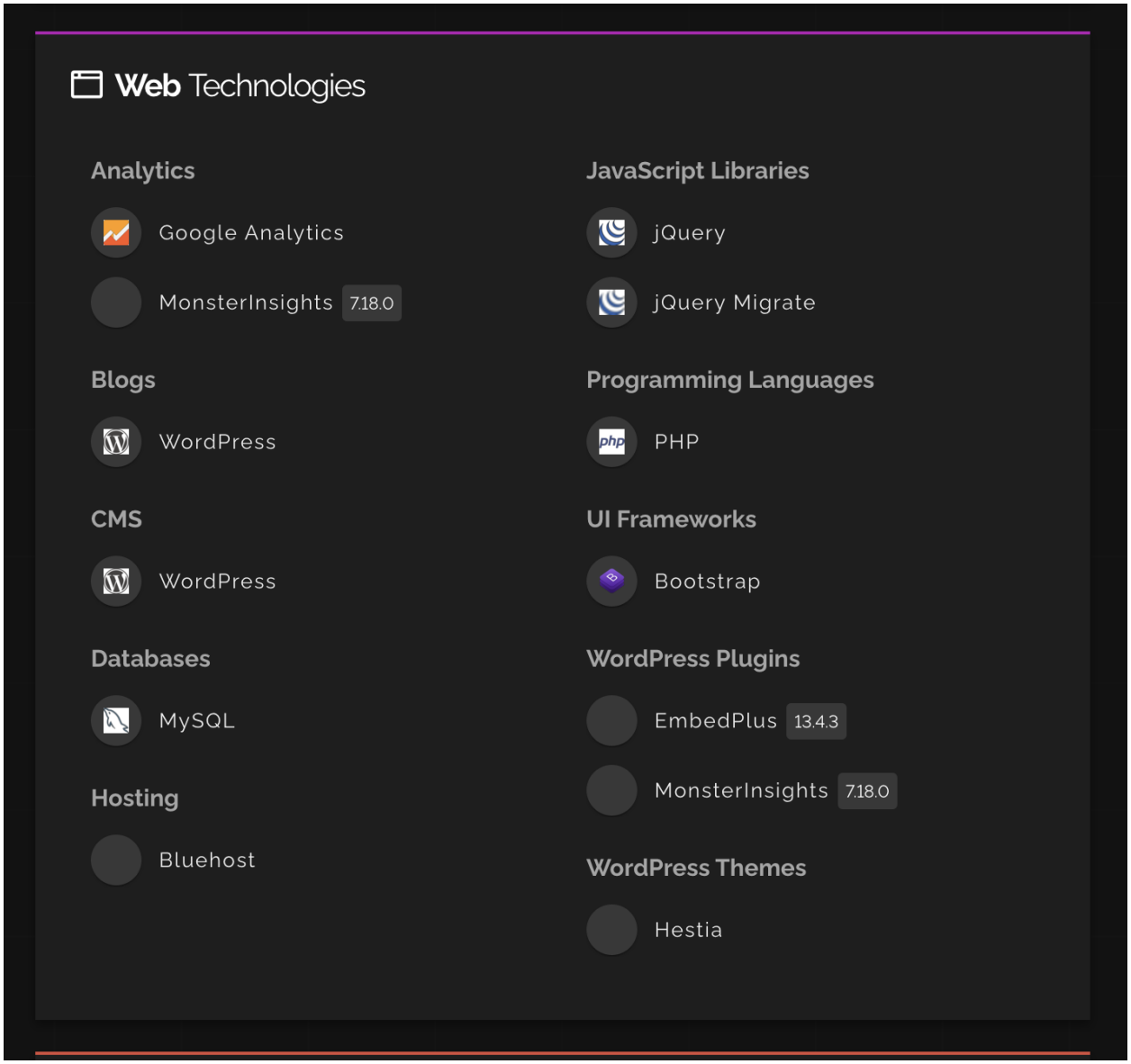
Cmd : knockpy certifiedhacker.com

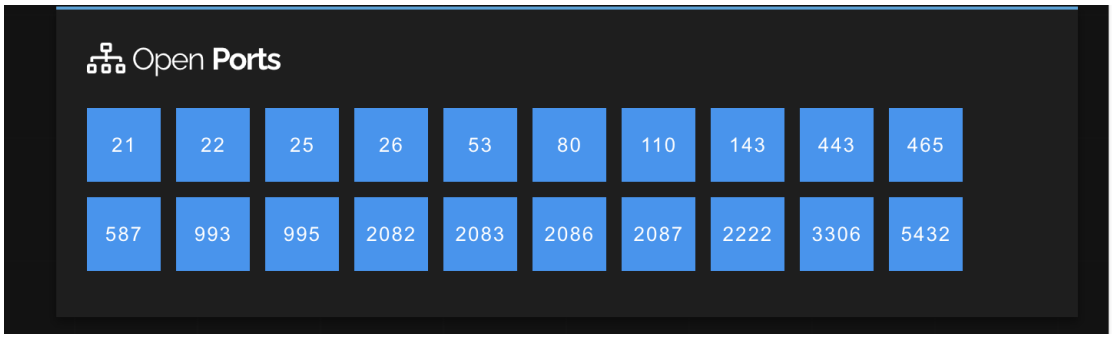


Shodan.io

Shodan (Sentient Hyper-Optimised Data Access Network) is a search engine designed to map and gather information about internet-connected devices and systems. Shodan.io is a legal website to search for open ports and vulnerabilities in a domain.


162.241.216.11
Regular View
Raw Data
// TAGS: database eol-product starttls
General Information
Hostnames
bluehost.com
box5331.bluehost.com
creativepathways.com
cpanel.creativepathways.com
cpcalendars.creativepathways.com
cpcontacts.creativepathways.com
mail.creativepathways.com
webdisk.creativepathways.com
webmail.creativepathways.com
www.creativepathways.com
Domains
BLUEHOST.COM
CREATIVEPATHWAYS.COM
Country
United States
City
San Francisco
Organization
Unified Layer
ISP
Unified Layer
ASN
AS46606





Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2023-38408	The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009.
CVE-2021-41617	4.4 sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.
CVE-2021-36368	2.6 ** DISPUTED ** An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is "this is not an authentication bypass, since nothing is being bypassed."
CVE-2020-15778	6.8 ** DISPUTED ** scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."

CVE-2020-14145	4.3 The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.
CVE-2019-6111	5.8 An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).
CVE-2019-6110	4.0 In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.
CVE-2019-6109	4.0 An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.
CVE-2018-20685	2.6 In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.

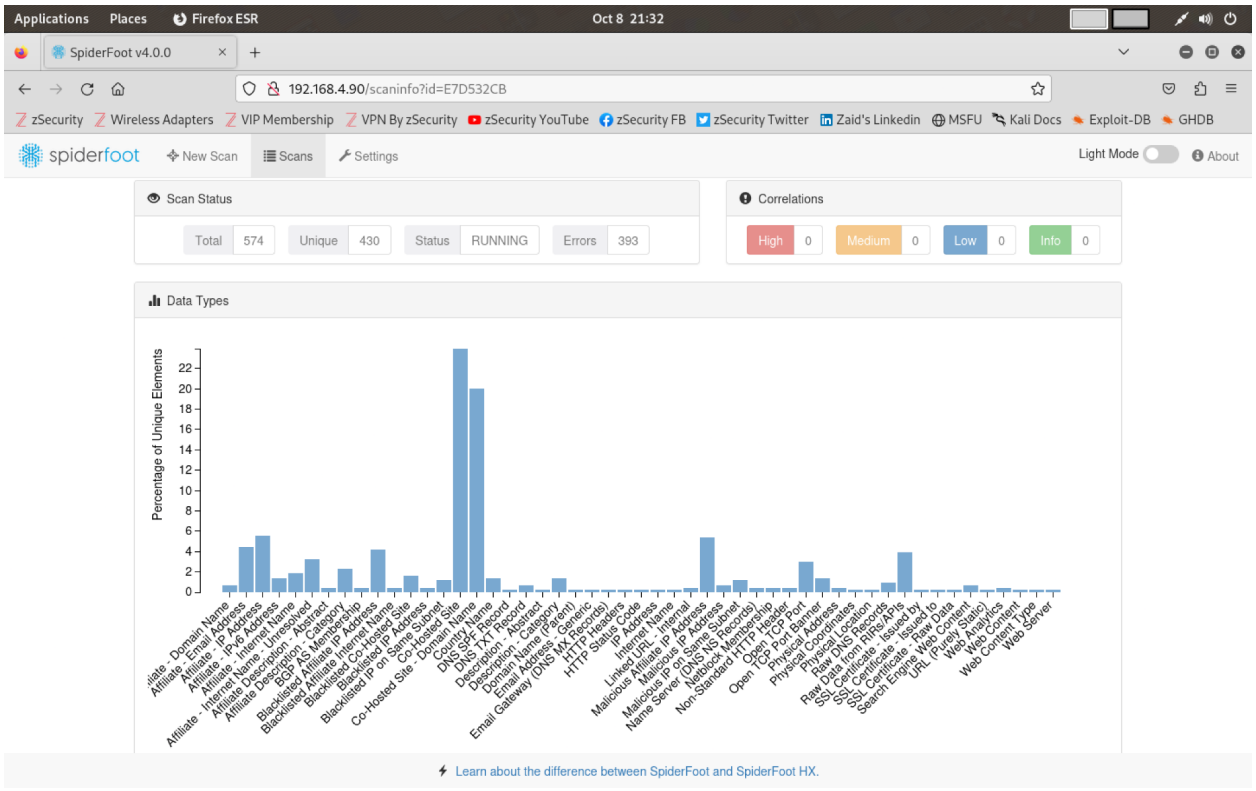
CVE-2018-20685	2.6 In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.
CVE-2018-15919	5.0 Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'
CVE-2018-15473	5.0 OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.
CVE-2017-15906	5.0 The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.
CVE-2016-20012	4.3 ** DISPUTED ** OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product.

Spiderfoot

SpiderFoot is an open-source intelligence (OSINT) automation tool designed for reconnaissance, information gathering, and footprinting of various online entities, such as websites, IP addresses, email addresses, and more.

Spiderfoot -l <ip address of the device and the port number 80>

The above command will start the local HTTP server for Spiderfoot which can be accessed through the IP address.



Nmap

Nmap, short for "Network Mapper," is a popular open-source network scanning and security auditing tool. It's used for network discovery, vulnerability scanning, and network security assessments. Nmap allows you to explore network hosts, discover open ports and services, gather information about those services, and even identify potential security vulnerabilities.

Cmd: nmap -p- -sV -O -T4 <ip address>
-p-: scan for all open ports
-sV: gives the version number
-O: gives the operating system
-T4: sets the timing template to speed up the scan

Exploits and vulnerabilities

Cmd: Nmap –script vuln <ip address>
–script: allows you to run a script
Vuln: a popular vulnerability scanning script

The open ports found on an Nmap scan are then referenced by Vulnerability databases like CVE, NVD, CWE, and CAPEC to find vulnerabilities associated with it.

Port 21

CVE-ID	
CVE-2020-10288	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
IRC5 exposes an ftp server (port 21). Upon attempting to gain access you are challenged with a request of username and password, however you can input whatever you like. As long as the field isn't empty it will be accepted.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• CONFIRM:https://github.com/aliasrobotics/RVD/issues/3327 • URL:https://github.com/aliasrobotics/RVD/issues/3327	
Assigning CNA	
Alias Robotics S.L.	
Date Record Created	
20200310	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20200310)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	
This is an record on the CVE List, which provides common identifiers for publicly known cybersecurity vulnerabilities.	

CVE-ID	
CVE-2018-10070	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
A vulnerability in MikroTik Version 6.41.4 could allow an unauthenticated remote attacker to exhaust all available CPU and all available RAM by sending a crafted FTP request on port 21 that begins with many '\0' characters, preventing the affected router from accepting new FTP connections. The router will reboot after 10 minutes, logging a "router was rebooted without proper shutdown" message.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• EXPLOIT-DB:44450 • URL:https://www.exploit-db.com/exploits/44450/ • MISC:http://packetstormsecurity.com/files/147183/MikroTik-6.41.4-Denial-Of-Service.html	
Assigning CNA	
MITRE Corporation	
Date Record Created	
20180412	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20180412)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	
This is an record on the CVE List, which provides common identifiers for publicly known cybersecurity vulnerabilities.	

Port 22

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.4 (protocol 2.0)
|_ssh-auth-methods: ERROR: Script execution failed (use -d to debug)
|_ssh-brute: ERROR: Script execution failed (use -d to debug)
| vulners:
|   cpe:/a:openbsd:openssh:7.4:
|       EXPLOITPACK:98FE96309F9524B8C84C508837551A19    5.8     https://vulners.com/exploitpack/EXPLOITPACK:98FE96309F9524B8C84C508837551A19    *EXPLOIT*
|       EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97    5.8     https://vulners.com/exploitpack/EXPLOITPACK:5330EA02EBDE345BFC9D6DDDD97F9E97    *EXPLOIT*
|       EDB-ID:46516    5.8     https://vulners.com/exploitdb/EDB-ID:46516      *EXPLOIT*
|       EDB-ID:46193    5.8     https://vulners.com/exploitdb/EDB-ID:46193      *EXPLOIT*
|       CVE-2019-6111   5.8     https://vulners.com/cve/CVE-2019-6111
|       1337DAY-ID-32328        5.8     https://vulners.com/zdt/1337DAY-ID-32328        *EXPLOIT*
|       1337DAY-ID-32009        5.8     https://vulners.com/zdt/1337DAY-ID-32009        *EXPLOIT*
|       SSH_ENUM        5.0     https://vulners.com/canvas/SSH_ENUM     *EXPLOIT*
|       PACKETSTORM:150621      5.0     https://vulners.com/packetstorm/PACKETSTORM:150621      *EXPLOIT*
|       EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0    5.0     https://vulners.com/exploitpack/EXPLOITPACK:F957D7E8A0CC1E23C3C649B764E13FB0    *EXPLOIT*
|       EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283    5.0     https://vulners.com/exploitpack/EXPLOITPACK:EBDBC5685E3276D648B4D14B75563283    *EXPLOIT*
|       EDB-ID:45939    5.0     https://vulners.com/exploitdb/EDB-ID:45939      *EXPLOIT*
|       EDB-ID:45233    5.0     https://vulners.com/exploitdb/EDB-ID:45233      *EXPLOIT*
|       CVE-2018-15919  5.0     https://vulners.com/cve/CVE-2018-15919
|       CVE-2018-15473  5.0     https://vulners.com/cve/CVE-2018-15473
|       CVE-2017-15906  5.0     https://vulners.com/cve/CVE-2017-15906
|       CVE-2016-10708  5.0     https://vulners.com/cve/CVE-2016-10708
|       1337DAY-ID-31730        5.0     https://vulners.com/zdt/1337DAY-ID-31730        *EXPLOIT*
|       CVE-2021-41617  4.4     https://vulners.com/cve/CVE-2021-41617
|       CVE-2020-14145  4.3     https://vulners.com/cve/CVE-2020-14145
|       CVE-2019-6110   4.0     https://vulners.com/cve/CVE-2019-6110
|       CVE-2019-6109   4.0     https://vulners.com/cve/CVE-2019-6109
|       CVE-2018-20685  2.6     https://vulners.com/cve/CVE-2018-20685
|       PACKETSTORM:151227      0.0     https://vulners.com/packetstorm/PACKETSTORM:151227      *EXPLOIT*
|       MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS-        0.0     https://vulners.com/metasploit/MSF:AUXILIARY-SCANNER-SSH-SSH_ENUMUSERS- *EXPLOIT*
|_      1337DAY-ID-30937        0.0     https://vulners.com/zdt/1337DAY-ID-30937        *EXPLOIT*
|_ssh-publickey-acceptance: ERROR: Script execution failed (use -d to debug)
|_ssh-run: ERROR: Script execution failed (use -d to debug)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.4 (93%), Linux 2.6.18 (89%), Linux 2.6.32 (88%), Linux 3.5 (88%), Linux 3.7 (88%), Linux 4.2 (88%), Linux 4.4 (88%), Synology DiskStation Manager 5.1 (88%), WatchGuard Fire
ware 11.8 (88%), Linux 3.2.0 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 12 hops
```

CVE-ID	
CVE-2023-43631	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

On boot, the Pillar eve container checks for the existence and content of “/config/authorized_keys”. If the file is present, and contains a supported public key, the container will go on to open port 22 and enable sshd with the given keys as the authorized keys for root login. An attacker could easily add their own keys and gain full control over the system without triggering the “measured boot” mechanism implemented by EVE OS, and without marking the device as “UUD” (“Unknown Update Detected”). This is because the “/config” partition is not protected by “measured boot”, it is mutable, and it is not encrypted in any way. An attacker can gain full control over the device without changing the PCR values, thus not triggering the “measured boot” mechanism, and having full access to the vault. Note: This issue was partially fixed in these commits (after disclosure to Zededa), where the config partition measurement was added to PCR13: • aa3501d6c57206ced222c33aea15a9169d629141 • 5fef4d92e75838cc78010edaed5247dfbdae1889. This issue was made viable in version 9.0.0 when the calculation was moved to PCR14 but it was not included in the measured boot.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://asrg.io/security-advisories/cve-2023-43631/
- URL:https://asrg.io/security-advisories/cve-2023-43631/

Assigning CNA

Automotive Security Research Group (ASRG)

Date Record Created

20230920	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20230920)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

This is an record on the CVE List, which provides common identifiers for publicly known cybersecurity vulnerabilities.

SEARCH CVE USING KEYWORDS: Submit

You can also search by reference using the CVE Reference Maps.

CVE-ID	
CVE-2022-30318	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
Honeywell ControlEdge through R151.1 uses Hard-coded Credentials. According to FSCT-2022-0056, there is a Honeywell ControlEdge hardcoded credentials issue. The affected components are characterized as: SSH. The potential impact is: Remote code execution, manipulate configuration, denial of service. The Honeywell ControlEdge PLC and RTU product line exposes an SSH service on port 22/TCP. Login as root to this service is permitted and credentials for the root user are hardcoded without automatically changing them upon first commissioning. The credentials for the SSH service are hardcoded in the firmware. The credentials grant an attacker access to a root shell on the PLC/RTU, allowing for remote code execution, configuration manipulation and denial of service.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• MISC:https://www.cisa.gov/uscert/ics/advisories/icsa-22-242-06 • MISC:https://www.forescout.com/blog/	
Assigning CNA	
MITRE Corporation	
Date Record Created	
20220506	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20220506)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	

Port 25

CVE-ID	
CVE-2021-43270	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
Datalust Seq.App.EmailPlus (aka seq-app-htmlemail) 3.1.0-dev-00148, 3.1.0-dev-00170, and 3.1.0-dev-00176 can use cleartext SMTP on port 25 in some cases where encryption on port 465 was intended.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• MISC:https://github.com/datalust/seq-app-htmlemail/pull/93	
Assigning CNA	
MITRE Corporation	
Date Record Created	
20211102	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20211102)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	

CVE-ID	
CVE-2010-1103	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Integer overflow in Stainless allows remote attackers to bypass intended port restrictions on outbound TCP connections via a port number outside the range of the unsigned short data type, as demonstrated by a value of 65561 for TCP port 25.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BUGTRAQ:20100323 Safari browser port blocking bypassed by integer overflow
- URL:http://www.securityfocus.com/archive/1/510283/100/0/threaded
- XF:stainless-tcp-security-bypass(57237)
- URL:https://exchange.xforce.ibmcloud.com/vulnerabilities/57237

Assigning CNA

MITRE Corporation

Date Record Created

20100324	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20100324)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

Port 26

CWE-787: Out-of-bounds Write

Weakness ID: 787
Abstraction: Base
Structure: Simple

View customized information: Conceptual | Operational | Mapping Friendly | **Complete** | Custom

Description

The product writes data past the end, or before the beginning, of the intended buffer.

Extended Description

Typically, this can result in corruption of data, a crash, or code execution. The product may modify an index or perform pointer arithmetic that references a memory location that is outside of the boundaries of the buffer. A subsequent write operation then produces undefined or unexpected results.

Alternate Terms

Memory Corruption: Often used to describe the consequences of writing to memory outside the bounds of a buffer, or to memory that is invalid, when the root cause is something other than a sequential copy of excessive data from a fixed starting location. This may include issues such as incorrect pointer arithmetic, accessing invalid pointers due to incomplete initialization or memory release, etc.

Relationships

Relevant to the view "Research Concepts" (CWE-1000)

Nature	Type	ID	Name
ChildOf	C	119	Improper Restriction of Operations within the Bounds of a Memory Buffer
ParentOf	V	121	Stack-based Buffer Overflow
ParentOf	V	122	Heap-based Buffer Overflow
ParentOf	B	123	Write-what-where Condition
ParentOf	B	124	Buffer Underwrite ('Buffer Underflow')
CanFollow	B	822	Untrusted Pointer Dereference
CanFollow	B	823	Use of Out-of-range Pointer Offset
CanFollow	B	824	Access of Uninitialized Pointer
CanFollow	B	825	Expired Pointer Dereference

Relevant to the view "Software Development" (CWE-699)

Nature	Type	ID	Name
MemberOf	C	1218	Memory Buffer Errors

Relevant to the view "Weaknesses for Simplified Mapping of Published Vulnerabilities" (CWE-1003)
Relevant to the view "CISQ Quality Measures (2020)" (CWE-1305)
Relevant to the view "CISQ Data Protection Measures" (CWE-1340)

Port 53

```
PORT   STATE SERVICE VERSION
53/tcp open  domain  ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
| dns-nsid:
|_  bind.version: 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9
| dns-nsec-enum:
|_  No NSEC records found
| dns-nsec3-enum:
|_  DNSSEC NSEC3 not supported
| vulners:
|   cpe:/o:redhat:enterprise_linux:7:
|       SSV:93135       10.0    https://vulners.com/seebug/SSV:93135    *EXPLOIT*
|       SSV:92513       10.0    https://vulners.com/seebug/SSV:92513    *EXPLOIT*
|       SSV:92510       10.0    https://vulners.com/seebug/SSV:92510    *EXPLOIT*
|       SSV:92405       10.0    https://vulners.com/seebug/SSV:92405    *EXPLOIT*
|       SSV:89724       10.0    https://vulners.com/seebug/SSV:89724    *EXPLOIT*
|       PACKETSTORM:165816      10.0    https://vulners.com/packetstorm/PACKETSTORM:165816      *EXPLOIT*
|       PACKETSTORM:143369      10.0    https://vulners.com/packetstorm/PACKETSTORM:143369      *EXPLOIT*
|       PACKETSTORM:139491      10.0    https://vulners.com/packetstorm/PACKETSTORM:139491      *EXPLOIT*
|       PACKETSTORM:139476      10.0    https://vulners.com/packetstorm/PACKETSTORM:139476      *EXPLOIT*
|       PACKETSTORM:138678      10.0    https://vulners.com/packetstorm/PACKETSTORM:138678      *EXPLOIT*
|       EXPLOITPACK:D127040CBAC5DBD24F717F40D86D1AF6    10.0    https://vulners.com/exploitpack/EXPLOITPACK:D127040CBAC5DBD24F717F40D86D1AF6    *EXPLOIT*
|       EXPLOITPACK:BD83B747C6C6A417D97824A1D81FAA5D    10.0    https://vulners.com/exploitpack/EXPLOITPACK:BD83B747C6C6A417D97824A1D81FAA5D    *EXPLOIT*
|       EXPLOITPACK:55F22FE44A0D6F3F9005C334804B2317    10.0    https://vulners.com/exploitpack/EXPLOITPACK:55F22FE44A0D6F3F9005C334804B2317    *EXPLOIT*
|       EXPLOITPACK:3D8D46697DAADEA8249E37B2A2F09AE3    10.0    https://vulners.com/exploitpack/EXPLOITPACK:3D8D46697DAADEA8249E37B2A2F09AE3    *EXPLOIT*
|       EXPLOITPACK:069C31B8DD5A351921E9625221546 6D8   10.0    https://vulners.com/exploitpack/EXPLOITPACK:069C31B8DD5A351921E9625221546 6D8   *EXPLOIT*
|       EDB-ID:50691    10.0    https://vulners.com/exploitdb/EDB-ID:50691      *EXPLOIT*
|       EDB-ID:42091    10.0    https://vulners.com/exploitdb/EDB-ID:42091      *EXPLOIT*
|       EDB-ID:40679    10.0    https://vulners.com/exploitdb/EDB-ID:40679      *EXPLOIT*
|       EDB-ID:40678    10.0    https://vulners.com/exploitdb/EDB-ID:40678      *EXPLOIT*
|       EDB-ID:40360    10.0    https://vulners.com/exploitdb/EDB-ID:40360      *EXPLOIT*
|       EDB-ID:36741    10.0    https://vulners.com/exploitdb/EDB-ID:36741      *EXPLOIT*
|       CVE-2021-3466   10.0    https://vulners.com/cve/CVE-2021-3466
|       CVE-2018-14618  10.0    https://vulners.com/cve/CVE-2018-14618
|       CVE-2016-6662   10.0    https://vulners.com/cve/CVE-2016-6662
|       CVE-2016-0639   10.0    https://vulners.com/cve/CVE-2016-0639
|       CVE-2015-4603   10.0    https://vulners.com/cve/CVE-2015-4603
|       CVE-2015-4602   10.0    https://vulners.com/cve/CVE-2015-4602
|       CVE-2015-0408   10.0    https://vulners.com/cve/CVE-2015-0408
|       CVE-2015-0240   10.0    https://vulners.com/cve/CVE-2015-0240
|       CVE-2014-6601   10.0    https://vulners.com/cve/CVE-2014-6601
|       CVE-2014-3585   10.0    https://vulners.com/cve/CVE-2014-3585
|       CVE-2011-2767   10.0    https://vulners.com/cve/CVE-2011-2767
```

CVE-ID	
CVE-2018-19528	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
TP-Link TL-WR886N 7.0 1.1.0 devices allow remote attackers to cause a denial of service (Tlb Load Exception) via crafted DNS packets to port 53/udp.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• MISC:https://github.com/PAGalaxyLab/VulInfo/blob/master/TP-Link/WR886N/dns_request_buff_overflow/README.md	
Assigning CNA	
MITRE Corporation	
Date Record Created	
20181125	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20181125)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	

CVE-ID	
CVE-2017-17537	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
MikroTik RouterBOARD v6.39.2 and v6.40.5 allows an unauthenticated remote attacker to cause a denial of service by connecting to TCP port 53 and sending data that begins with many '\0' characters, possibly related to DNS.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• EXPLOIT-DB:43200 • URL:https://www.exploit-db.com/exploits/43200/	
Assigning CNA	
MITRE Corporation	
Date Record Created	
20171211	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20171211)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	

Port 80

CVE-ID	
CVE-2022-47040	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
An issue in ASKEY router RTF3505VW-N1 BR_SV_g000_R3505VMN1001_s32_7 allows attackers to escalate privileges via running the tcpdump command after placing a crafted file in the /tmp directory and sending crafted packets through port 80.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• MISC:https://github.com/leoservalli/Privilege-escalation-ASKEY	
Assigning CNA	
MITRE Corporation	
Date Record Created	
20221212	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20221212)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	

CVE-ID	
CVE-2022-43636	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of TP-Link TL-WR940N 6_211111 3.20.1(US) routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the httpd service, which listens on TCP port 80 by default. The issue results from the lack of sufficient randomness in the sequnce numbers used for session managment. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-18334.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• MISC:https://www.zerodayinitiative.com/advisories/ZDI-22-1614/ • URL:https://www.zerodayinitiative.com/advisories/ZDI-22-1614/	
Assigning CNA	
Zero Day Initiative	
Date Record Created	
20221021	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20221021)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	

Port 110

CVE-2010-0816	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
Integer overflow in inetcomm.dll in Microsoft Outlook Express 5.5 SP2, 6, and 6 SP1; Windows Live Mail on Windows XP SP2 and SP3, Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7; and Windows Mail on Windows Vista SP1 and SP2, Windows Server 2008 Gold, SP2, and R2, and Windows 7 allows remote e-mail servers and man-in-the-middle attackers to execute arbitrary code via a crafted (1) POP3 or (2) IMAP response, as demonstrated by a certain +OK response on TCP port 110, aka "Outlook Express and Windows Mail Integer Overflow Vulnerability."	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• BID:40052 • URL:http://www.securityfocus.com/bid/40052 • BUGTRAQ:20100511 {PRL} Microsoft Windows Outlook Express and Windows Mail Integer Overflow • URL:http://archives.neohapsis.com/archives/bugtraq/2010-05/0068.html • CERT:TA10-131A • URL:http://www.us-cert.gov/cas/techalerts/TA10-131A.html • MISC:http://www.protekresearchlab.com/index.php?option=com_content&view=article&id=13&Itemid=13 • MS:MS10-030 • URL:https://docs.microsoft.com/en-us/security-updates/securitybulletins/2010/ms10-030 • OVAL:oval:org.mitre.oval:def:6734 • URL:https://oval.cisecurity.org/repository/search/definition/oval%3Aorg.mitre.oval%3Adef%3A6734	
Assigning CNA	
Microsoft Corporation	
Date Record Created	
20100302	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20100302)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	

CVE-ID	
CVE-2007-5467	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
Integer overflow in eXtremail 2.1.1 and earlier allows remote attackers to cause a denial of service, and possibly execute arbitrary code, via a long USER command containing "%s" sequences to the pop3 port (110/tcp), which are expanded to "%%s" before being used in the memmove function, possibly due to an incomplete fix for CVE-2001-1078.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• BID:26074 • URL:http://www.securityfocus.com/bid/26074 • BUGTRAQ:20071015 eXtremail(ly easy) remote roots • URL:http://www.securityfocus.com/archive/1/482293 • EXPLOIT-DB:4532 • URL:https://www.exploit-db.com/exploits/4532 • MISC:http://www.digit-labs.org/files/exploits/extremail-v3.pl • SECUNIA:27220 • URL:http://secunia.com/advisories/27220	
Assigning CNA	
MITRE Corporation	
Date Record Created	
20071015	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20071015)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	

Port 113

CVE-ID	
CVE-2007-2711	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
Stack-based buffer overflow in TinyIdentD 2.2 and earlier allows remote attackers to execute arbitrary code via a long string to TCP port 113.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• BID:23981 • URL:http://www.securityfocus.com/bid/23981 • EXPLOIT-DB:3925 • URL:https://www.exploit-db.com/exploits/3925 • OSVDB:36053 • URL:~~http://osvdb.org/36053~~ (Obsolete source) • SECUNIA:25248 • URL:http://secunia.com/advisories/25248 • VUPEN:ADV-2007-1825 • URL:~~http://www.vupen.com/english/advisories/2007/1825~~ (Obsolete source) • XF:tinyidentd-identification-bo(34298) • URL:https://exchange.xforce.ibmcloud.com/vulnerabilities/34298	
Assigning CNA	
MITRE Corporation	
Date Record Created	
20070515	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20070515)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	

Port 143

CVE-ID	
CVE-2009-0671	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

** REJECT ** Format string vulnerability in the University of Washington (UW) c-client library, as used by the UW IMAP toolkit imap-2007d and other applications, allows remote attackers to execute arbitrary code via format string specifiers in the initial request to the IMAP port (143/tcp). NOTE: Red Hat has disputed the vulnerability, stating "The Red Hat Security Response Team have been unable to confirm the existence of this format string vulnerability in the toolkit, and the sample published exploit is not complete or functional." CVE agrees that the exploit contains syntax errors and uses Unix-only include files while invoking Windows functions.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BID:33795
- URL:http://www.securityfocus.com/bid/33795
- MISC:http://packetstormsecurity.org/0902-exploits/uwimap-format.txt
- MISC:http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-0671
- VIM:20090224 possibly false: CVE-2009-0671 (IMAP c-client format string)
- URL:http://www.attrition.org/pipermail/vim/2009-February/002147.html
- VIM:20090224 possibly false: CVE-2009-0671 (IMAP c-client format string)
- URL:http://www.attrition.org/pipermail/vim/2009-February/002148.html
- XF:imap-toolkit-cclient-format-string(48798)
- URL:https://exchange.xforce.ibmcloud.com/vulnerabilities/48798

Assigning CNA

MITRE Corporation

Date Record Created

20090222	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20090222)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

CVE-ID	
CVE-2008-1713	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

MailServer.exe in NoticeWare Email Server 4.6.1.0 allows remote attackers to cause a denial of service (application crash) via a long string to IMAP port (143/tcp).

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BID:28559
- URL:http://www.securityfocus.com/bid/28559
- EXPLOIT-DB:5341
- URL:https://www.exploit-db.com/exploits/5341
- SECUNIA:29629
- URL:http://secunia.com/advisories/29629
- XF:emailserverng-mailserver-dos(41581)
- URL:https://exchange.xforce.ibmcloud.com/vulnerabilities/41581

Assigning CNA

MITRE Corporation

Date Record Created

20080409	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20080409)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

Port 443

CVE-ID	
CVE-2023-28489	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
A vulnerability has been identified in CP-8031 MASTER MODULE (All versions < CPCI85 V05), CP-8050 MASTER MODULE (All versions < CPCI85 V05). Affected devices are vulnerable to command injection via the web server port 443/tcp, if the parameter “Remote Operation” is enabled. The parameter is disabled by default. The vulnerability could allow an unauthenticated remote attacker to perform arbitrary code execution on the device.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• FULLDISC:20230707 SEC Consult SA-20230703-0 :: Multiple Vulnerabilities including Unauthenticated RCE in Siemens A8000 • URL:http://seclists.org/fulldisclosure/2023/Jul/14 • MISC:http://packetstormsecurity.com/files/173370/Siemens-A8000-CP-8050-CP-8031-Code-Execution-Command-Injection.html • MISC:https://cert-portal.siemens.com/productcert/pdf/ssa-472454.pdf • URL:https://cert-portal.siemens.com/productcert/pdf/ssa-472454.pdf	
Assigning CNA	
Siemens	
Date Record Created	
20230316	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20230316)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	

CVE-ID	
CVE-2023-0595	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
A CWE-117: Improper Output Neutralization for Logs vulnerability exists that could cause the misinterpretation of log files when malicious packets are sent to the Geo SCADA server's database web port (default 443). Affected products: EcoStruxure Geo SCADA Expert 2019, EcoStruxure Geo SCADA Expert 2020, EcoStruxure Geo SCADA Expert 2021(All Versions prior to October 2022), ClearSCADA (All Versions)	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• MISC:https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-045-01&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-01.pdf • URL:https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2023-045-01&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2023-045-01.pdf	
Assigning CNA	
Schneider Electric SE	
Date Record Created	
20230131	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20230131)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	

Port 465

CVE-ID	
CVE-2011-4015	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
Cisco IOS 15.2S allows remote attackers to cause a denial of service (interface queue wedge) via malformed UDP traffic on port 465, aka Bug ID CSCts48300.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• CONFIRM:http://www.cisco.com/en/US/docs/ios/15_2s/release/notes/15_2s_caveats_15_2_2s.html • SECTRACK:1027005 • URL:http://www.securitytracker.com/id?1027005	
Assigning CNA	
Cisco Systems, Inc.	
Date Record Created	
20111006	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20111006)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	

Port 2222

CVE-ID	
CVE-2018-18388	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
eScan Agent Application (MWAGENT.EXE) 4.0.2.98 in MicroWorld Technologies eScan 14.0 allows remote or local attackers to execute arbitrary commands by sending a carefully crafted payload to TCP port 2222.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• CONFIRM:http://blog.escanav.com/2018/11/cve-2018-18388/	
Assigning CNA	
MITRE Corporation	
Date Record Created	
20181016	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20181016)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	

CVE-ID	
CVE-2007-0655	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

The MicroWorld Agent service (MWAGENT.EXE) in MicroWorld Technologies eScan 8.0.671.1, and possibly other versions, allows remote or local attackers to gain privileges and execute arbitrary commands by connecting directly to TCP port 2222.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BID:23759
- URL:http://www.securityfocus.com/bid/23759
- MISC:http://secunia.com/secunia_research/2007-45/advisory/
- OSVDB:35732
- URL:~~http://osvdb.org/35732~~ (Obsolete source)
- SECTRACK:1018007
- URL:http://www.securitytracker.com/id?1018007
- SECUNIA:23809
- URL:http://secunia.com/advisories/23809
- VUPEN:ADV-2007-1609
- URL:~~http://www.vupen.com/english/advisories/2007/1609~~ (Obsolete source)
- XF:escan-mwagent-security-bypass(34009)
- URL:https://exchange.xforce.ibmcloud.com/vulnerabilities/34009

Assigning CNA

Flexera Software LLC

Date Record Created

20070201	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20070201)

Port 3306

```
PORT     STATE SERVICE VERSION
3306/tcp open  mysql   MySQL 5.7.23-23
| mysql-enum:
|   Valid usernames:
|     root:<empty> - Valid credentials
|     netadmin:<empty> - Valid credentials
|     guest:<empty> - Valid credentials
|     user:<empty> - Valid credentials
|     web:<empty> - Valid credentials
|     sysadmin:<empty> - Valid credentials
|     administrator:<empty> - Valid credentials
|     webadmin:<empty> - Valid credentials
|     admin:<empty> - Valid credentials
|     test:<empty> - Valid credentials
|_  Statistics: Performed 10 guesses in 1 seconds, average tps: 10.0
| mysql-brute:
|   Accounts: No valid accounts found
|   Statistics: Performed 0 guesses in 1 seconds, average tps: 0.0
|_  ERROR: The service seems to have failed or is heavily firewalled...
| mysql-info:
|   Protocol: 10
|   Version: 5.7.23-23
|   Thread ID: 5405863
|   Capabilities flags: 65535
|   Some Capabilities: Support41Auth, SupportsLoadDataLocal, Speaks41ProtocolNew, ConnectWithDatabase, IgnoreSigpipes, FoundRows, LongPassword, InteractiveClient, IgnoreSpaceBeforeParenthesis, SwitchToSS
LAfterHandshake, SupportsCompression, LongColumnFlag, SupportsTransactions, Speaks41ProtocolOld, ODBCClient, DontAllowDatabaseTableColumn, SupportsMultipleResults, SupportsMultipleStatments, SupportsAuth
Plugins
|   Status: Autocommit
|   Salt: \x07|>\]\x15e9\x1A5\x05\x0E 5*?\x16Z+S
|_  Auth Plugin Name: mysql_native_password
|_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)
|_mysql-empty-password: ERROR: Script execution failed (use -d to debug)
| vulners:
|   cpe:/a:mysql:mysql:5.7.23-23:
|       PRION:CVE-2021-2011     7.1     https://vulners.com/prion/PRION:CVE-2021-2011
|       PRION:CVE-2021-2060     6.8     https://vulners.com/prion/PRION:CVE-2021-2060
|       PRION:CVE-2021-2014     6.8     https://vulners.com/prion/PRION:CVE-2021-2014
|       PRION:CVE-2021-2001     6.8     https://vulners.com/prion/PRION:CVE-2021-2001
|       PRION:CVE-2021-2144     6.5     https://vulners.com/prion/PRION:CVE-2021-2144
|       PRION:CVE-2021-2022     6.3     https://vulners.com/prion/PRION:CVE-2021-2022
|       PRION:CVE-2022-21367    5.5     https://vulners.com/prion/PRION:CVE-2022-21367
|       PRION:CVE-2021-2356     4.9     https://vulners.com/prion/PRION:CVE-2021-2356
|       PRION:CVE-2021-2010     4.9     https://vulners.com/prion/PRION:CVE-2021-2010
|       PRION:CVE-2023-21980    4.6     https://vulners.com/prion/PRION:CVE-2023-21980
|       PRION:CVE-2021-2007     4.3     https://vulners.com/prion/PRION:CVE-2021-2007
|       PRION:CVE-2022-21592    4.0     https://vulners.com/prion/PRION:CVE-2022-21592
|       PRION:CVE-2022-21589    4.0     https://vulners.com/prion/PRION:CVE-2022-21589
```

CVE-ID	
CVE-2023-5157	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
A vulnerability was found in MariaDB. An OpenVAS port scan on ports 3306 and 4567 allows a malicious remote client to cause a denial of service.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• MISC:RHBZ#2240246 • URL:https://bugzilla.redhat.com/show_bug.cgi?id=2240246 • MISC:https://access.redhat.com/security/cve/CVE-2023-5157 • URL:https://access.redhat.com/security/cve/CVE-2023-5157	
Assigning CNA	
Red Hat, Inc.	
Date Record Created	
20230925	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20230925)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	

CVE-ID	
CVE-2011-5049	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
MySQL 5.5.8, when running on Windows, allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted packet to TCP port 3306.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• EXPLOIT-DB:18269 • URL:http://www.exploit-db.com/exploits/18269 • XF:mysql-port-dos(71965) • URL:https://exchange.xforce.ibmcloud.com/vulnerabilities/71965	
Assigning CNA	
MITRE Corporation	
Date Record Created	
20120104	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20120104)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	

Port 5432

CVE-ID	
CVE-2006-6469	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
Xerox WorkCentre and WorkCentre Pro before 12.050.03.000, 13.x before 13.050.03.000, and 14.x before 14.050.03.000 do not block the postgres port (5432/tcp), which has unknown impact and remote attack vectors, probably related to unauthorized connections to a PostgreSQL daemon.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• CONFIRM:http://www.xerox.com/downloads/usa/en/c/cert_XRX06_004_v11.pdf • SECUNIA:23265 • URL:http://secunia.com/advisories/23265	
Assigning CNA	
MITRE Corporation	
Date Record Created	
20061211	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20061211)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	

Port 8080

CVE-ID	
CVE-2022-3323	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
An SQL injection vulnerability in Advantech iView 5.7.04.6469. The specific flaw exists within the ConfigurationServlet endpoint, which listens on TCP port 8080 by default. An unauthenticated remote attacker can craft a special column_value parameter in the setConfiguration action to bypass checks in com.imc.iview.utils.CUtils.checkSQLInjection() to perform SQL injection. For example, the attacker can exploit the vulnerability to retrieve the iView admin password.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• MISC:https://www.tenable.com/security/research/tra-2022-32 • URL:https://www.tenable.com/security/research/tra-2022-32	
Assigning CNA	
Tenable Network Security, Inc.	
Date Record Created	
20220926	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20220926)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	

CVE-ID	
CVE-2020-25232	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
A vulnerability has been identified in LOGO! 8 BM (incl. SIPLUS variants) (All versions < V8.3). Due to the usage of an insecure random number generation function and a deprecated cryptographic function, an attacker could extract the key that is used when communicating with an affected device on port 8080/tcp.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• MISC:https://cert-portal.siemens.com/productcert/pdf/ssa-480824.pdf • URL:https://cert-portal.siemens.com/productcert/pdf/ssa-480824.pdf	
Assigning CNA	
Siemens	
Date Record Created	
20200910	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20200910)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	

Port 8443

Description	
The Opportunistic Encryption feature of HTTP2 (RFC 8164) allows a connection to be transparently upgraded to TLS while retaining the visual properties of an HTTP connection, including being same-origin with unencrypted connections on port 80. However, if a second encrypted port on the same IP address (e.g. port 8443) did not opt-in to opportunistic encryption; a network attacker could forward a connection from the browser to port 443 to port 8443, causing the browser to treat the content of port 8443 as same-origin with HTTP. This was resolved by disabling the Opportunistic Encryption feature, which had low usage. This vulnerability affects Firefox < 94, Thunderbird < 91.3, and Firefox ESR < 91.3.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• DEBIAN:DSA-5026 • URL:https://www.debian.org/security/2021/dsa-5026 • DEBIAN:DSA-5034 • URL:https://www.debian.org/security/2022/dsa-5034 • GENTOO:GLSA-202202-03 • URL:https://security.gentoo.org/glsa/202202-03 • GENTOO:GLSA-202208-14 • URL:https://security.gentoo.org/glsa/202208-14 • MISC:https://bugzilla.mozilla.org/show_bug.cgi?id=1730935 • URL:https://bugzilla.mozilla.org/show_bug.cgi?id=1730935 • MISC:https://www.mozilla.org/security/advisories/mfsa2021-48/ • URL:https://www.mozilla.org/security/advisories/mfsa2021-48/ • MISC:https://www.mozilla.org/security/advisories/mfsa2021-49/ • URL:https://www.mozilla.org/security/advisories/mfsa2021-49/ • MISC:https://www.mozilla.org/security/advisories/mfsa2021-50/ • URL:https://www.mozilla.org/security/advisories/mfsa2021-50/ • MLIST:[debian-lts-announce] 20211229 [SECURITY] [DLA 2863-1] firefox-esr security update • URL:https://lists.debian.org/debian-lts-announce/2021/12/msg00030.html • MLIST:[debian-lts-announce] 20220104 [SECURITY] [DLA 2874-1] thunderbird security update • URL:https://lists.debian.org/debian-lts-announce/2022/01/msg00001.html	
Assigning CNA	
Mozilla Corporation	
Date Record Created	
20210810	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20210810)	

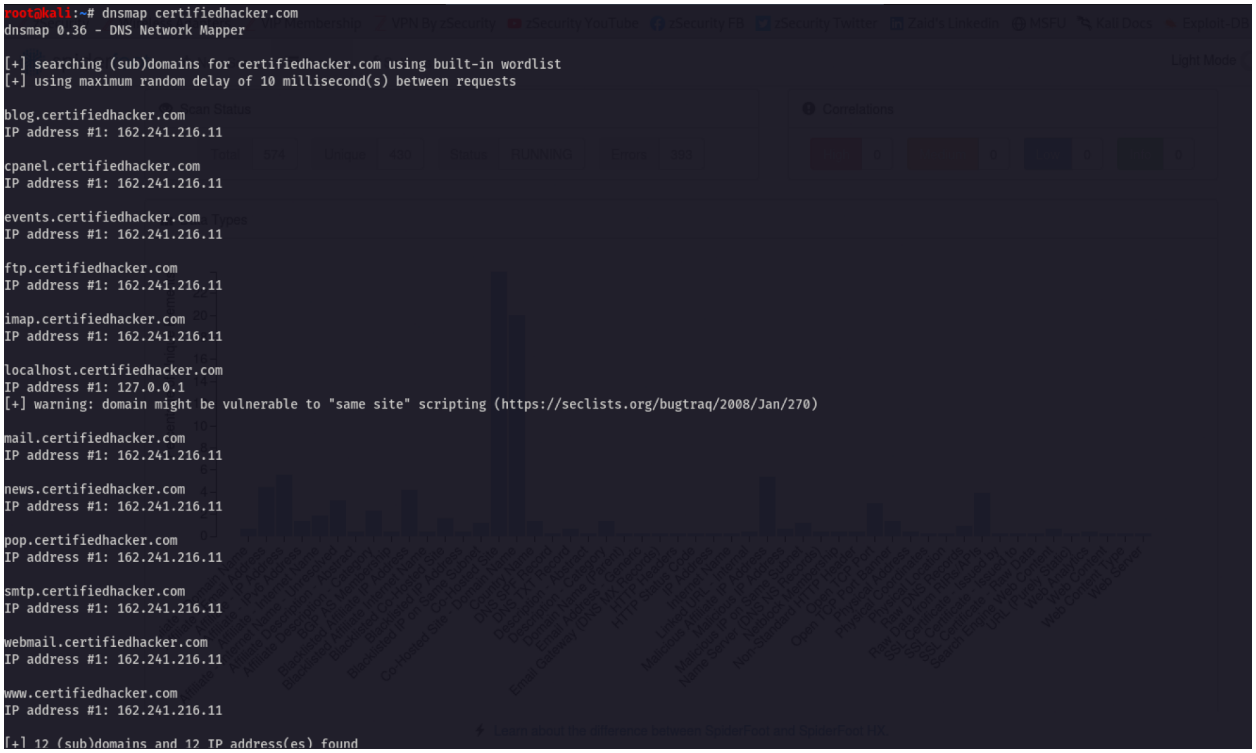
CVE-ID	
CVE-2021-22002	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
VMware Workspace ONE Access and Identity Manager, allow the /cfg web app and diagnostic endpoints, on port 8443, to be accessed via port 443 using a custom host header. A malicious actor with network access to port 443 could tamper with host headers to facilitate access to the /cfg web app, in addition a malicious actor could access /cfg diagnostic endpoints without authentication.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• MISC:https://www.vmware.com/security/advisories/VMSA-2021-0016.html • URL:https://www.vmware.com/security/advisories/VMSA-2021-0016.html	
Assigning CNA	
VMware	
Date Record Created	
20210104	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20210104)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	

CVE-ID	
CVE-2018-11716	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
An issue was discovered in Zoho ManageEngine Desktop Central before 100230. There is unauthenticated remote access to all log files of a Desktop Central instance containing critical information (private information such as location of enrolled devices, cleartext passwords, patching level, etc.) via a GET request on port 8022, 8443, or 8444.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• CONFIRM:https://www.manageengine.com/products/desktop-central/vulnerability-in-log-files.html • MISC:https://blog.netxp.fr/manageengine-deep-exploitation/	
Assigning CNA	
MITRE Corporation	
Date Record Created	
20180604	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20180604)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	

DNS map

DNS map is a command-line tool used for subdomain brute-forcing and mapping the DNS (Domain Name System) infrastructure of a target domain. It's primarily designed to discover subdomains associated with a specific domain by performing DNS queries and trying to identify

valid subdomains. DNS map can be useful for reconnaissance and information gathering during security assessments or penetration testing.



Summary

Using the above mentioned tools we were able to get a good insight of the website's makeup and infrastructure.

1) The domain was first deployed in 2002 and was still active with up to date technologies. But the technologies themselves are little outdated and are not updated that frequently.
2) The webserver has a lot of open ports which also has a number of vulnerabilities and exploits. We were able to find exploits that are too old which have not yet been patched up.
3) The Website has more than 10 subdomains and each of them are run on same server versions and have almost same name servers. This implies that the attacker can use the same methods and tools to exploit all the subdomains as they have similar infrastructure with same vulnerabilities

4) The Website runs on older versions of SSH/TLS from the year 2008. These outdated versions increase the chances of Man-in-the-middle attacks.
5) The website is missing essential security headers, such as Content Security Policy (CSP) and HTTP Strict Transport Security (HSTS), which are crucial for mitigating various web-based attacks.

Despite being vulnerable the website has some security features like firewall and HTTP secure to protect themselves from all kinds of basic attacks. This makes the website a beginner target for vulnerability analysis and pentesting. The website lacks a lot of features that you can find in modern day, up to date websites and domains. We got a lot of good tools to conduct reconnaissance, vulnerability analysis and pentesting.