

velocityrecoveries.com **www.velocityrecoveries.com**
141.193.213.20 141.193.213.20
141.193.213.21 141.193.213.21

675

 / 950

LAST SCANNED MAY 15 2026

FIRST SCANNED MAY 11 2020

This scan includes results from both velocityrecoveries.com and www.velocityrecoveries.com.

11 / 73 checks failed

Hostname does not match SSL certificate

velocityrecoveries.com:6443

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are mechanisms for securing traffic between two systems. They do this by using an encryption algorithm that makes the data unreadable for everyone except the two systems that possess the necessary certificates. These certificates provide a keypair, private and public, that is used to guarantee the encryption. Every certificate should include the preferred hostname(s) for the system that is being protected, so that the certificate can be verified to the address being accessed by the client.

When a certificate does not match the hostname the client is trying to access, it produces an error in the browser. This is because each certificate must specify the addresses for which it is valid. In addition to sites being rendered inaccessible to most browsers, mismatched certificates open the door for man-in-the-middle (MITM) attacks, as name confusion reduces the trustworthiness of all systems involved.

A new certificate should be requested from a trusted authority with the correct hostname(s) listed on it. This will prevent browser errors and reduce certificate complexity across the organization. All existing certificates should be audited to ensure that each one has the proper hostnames. Changes to hostnames or aliases should include steps to update certificates with the new names.

Expected	SSL > Host Match: [hostname matches SSL certificate]
Actual	velocityrecoveries.com does not match the Subject Alternative Name in the SSL certificate: nginx-cache
First detected	May 8, 2026

HTTP Strict Transport Security (HSTS) not enforced

velocityrecoveries.com:443

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are mechanisms for securing traffic between two systems. They do this by using an encryption algorithm that makes the data unreadable for everyone except the two systems that possess the necessary certificates. These certificates provide a keypair, private and public, that is used to guarantee the encryption. SSL/TLS uses the HTTPS protocol, so all client connections must be rerouted from HTTP to HTTPS when necessary. HTTP Strict Transport Security (HSTS) ensures that no HTTP connections will be allowed from the server. This forces the use of HTTPS, which maintains encryption at all times.

Without HSTS, servers are still allowed to establish unencrypted connections on the HTTP protocol. This can open the door for unexpected and unseen circumstances where a client passes sensitive information in plain text. HTTP to HTTPS redirects can still pass sensitive information, such as credentials in the URL, in plain text. This opens a window for a man-in-the-middle (MITM) attack. Old links that were overlooked might still specify HTTP. Users might create their own browser bookmarks using HTTP. As long as HTTP connections are possible, the risk of data interception is present.

Enable HSTS on the server. This is done by including the Strict-Transport-Security header on the system. The "includeSubDomains" directive should be specified to ensure all subdomains on the system use HTTPS. Submit your domain to Google's HSTS preload service. This preload list is included in most browsers and will automatically make all connections to the domain use an encrypted channel.

Expected	Headers > strict-transport-security: [header set]
Actual	[not set]
First detected	May 15, 2026

CSP is not implemented

velocityrecoveries.com:443

A Content-Security-Policy header defines directives for server governance on website behaviors through the HTTP header, though you can also supply HTML meta tags with a string-matching attribute that sets a CSP for the page. With your CSP, you define the approved origins for content that browsers will load on your website, such as JavaScript, CSS stylesheets, images, and more.

Without a CSP, malicious actors can inject their preferred content into your website, such as injecting a malicious script in a cross-site scripting attack or manipulating user behavior through a clickjacking attack. XSS attacks and UI redress are two attack vulnerabilities that could be exploited without a

Content Security Policy that defines authorized content sources.

To create the Content Security Policy for your website, you will need to update the configuration file containing your HTTP Response header. Different server setups and hosting platforms require different approaches to your configuration files. For example, you update the .htaccess or .httpd.conf files for Apache web servers, whereas NGINX servers require modification in the server block.

Expected	Headers > content-security-policy: [valid policy]
Actual	[not set]
First detected	May 15, 2026

DMARC policy is p=quarantine velocityrecoveries.com



Domain-based Message Authentication, Reporting and Conformance (DMARC) is an email security feature that works in conjunction with Sender Policy Framework (SPF) and/or DomainKeys Identified Mail (DKIM) to ensure that messages actually originate from the organizations claimed in the From: address. It does this by "aligning" the From: address with either the SPF or DKIM policy in the sender domain. If a message's From: address does not align with either of these policies, DMARC offers options on how to handle the message, including delivering it, quarantining it and blocking it altogether.

One of the most common phishing techniques is called email spoofing. Spoofing is when a malicious actor rewrites their email headers to make it seem as if the message is coming from a different, legitimate email domain. DMARC helps prevent spoofing by authenticating the From: address to the sender's domain. However, if DMARC is configured to use p=quarantine, it means that the fraudulent messages are still delivered to the destination email system. The destination system then determines how to handle quarantine procedures, depending on how it has been configured. This method should only be used temporarily to tweak DMARC/SPF before implementing a p=reject policy.

The p= value in DMARC provides instructions on what to do with an email that fails DMARC alignment. The p= value should ultimately be set to reject for best security; however, p=quarantine can be used temporarily to monitor DMARC behavior and ensure false positives are not being quarantined. Once this monitoring is complete, the p= value should be set to reject. This helps prevent fraudulent email from reaching end users.

Expected	DNS > DMARC: v=DMARC1; p=reject; ...
Actual	v=DMARC1;p=quarantine;sp=quarantine;pct=100;adkim=r;aspf=r;rua=mailto:tech@velocityrecoveries.com;ruf=mailto:tech@velocityrecoveries.com;fo=1
First detected	May 8, 2023

X-Content-Type-Options is not nosniff velocityrecoveries.com:443



The X-Content-Type-Options header is not set to "nosniff," an option that prevents MIME type sniffing. This header ensures that the content types defined in the Content-Type header are used and not changed.

Multipurpose Internet Mail Extension (MIME) content types are subject to content sniffing attacks, in which the attacker turns non-executable MIME types into executable MIME types. Without this option, an attacker may attempt cross-site scripting by uploading a non-executable content type (like an image) that contains script content that would be executed when another user accesses the file. The "nosniff" option ensures that content is only treated as an image and not script.

In the file that configures your server headers, add the header X-Content-Type-Options: nosniff. You should also ensure that the Content-Type is set correctly for the content you are expecting to server, and test that the site renders as desired after the change.

Expected	Headers > x-content-type-options: nosniff
Actual	[not set]
First detected	May 15, 2026

CAA not enabled velocityrecoveries.com www.velocityrecoveries.com



Certificate Authority Authorization (CAA) is a security mechanism that allows domain owners to specify which Certificate Authorities (CAs) are permitted to issue SSL/TLS certificates for their domain. The CAA policy is enforced through DNS (Domain Name System) records, providing an extra layer of security against unauthorized certificate issuance.

When a Certificate Authority receives a certificate request for a domain, it is required to check the domain's CAA records before issuing the certificate. Without a CAA, it is possible to have certificates issued for a domain by an unapproved certificate authority.

CAA is implemented as a DNS resource record (type CAA). Domain owners add CAA records to their DNS zone file, specifying which CAs are allowed to issue certificates for that domain. To allow Let's Encrypt to issue certificates, the record would look like: example.com. IN CAA 0 issue "letsencrypt.org".

Expected	CAA: [set]
----------	------------

Actual	[not set]
First detected	Nov 25, 2022

Weak cipher suites supported in TLS 1.2



velocityrecoveries.com:443
www.velocityrecoveries.com:443

Transport Layer Security (TLS) 1.2 supports several strong cipher suites, but also includes some that are considered obsolete or weak. Weak encryption algorithms in TLS 1.2 include NULL, RC2, RC4, DES, IDEA, and TDES/3DES, and cipher suites using these algorithms should not be used.

Supporting weak cipher suites in TLS 1.2 means that attackers can attempt to force the usage of these cipher suites, even when secure ciphers are also available. Exploiting weak cipher suites can be used by hackers to eavesdrop on communications, intercept data, and launch adversary-in-the-middle attacks.

TLS 1.3 no longer includes the weak cipher suites available in 1.2. Upgrading to 1.3 will resolve the issue. Within 1.2, compare the list of cipher suites in use to the list at ciphersuite.info/cs to identify which are insecure.

Expected	SSL > Supported Cipher Suite: [secure ciphers only]
Actual	TLSv1.2: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
First detected	May 24, 2023

'HTTP' port open



141.193.213.20
141.193.213.21

HTTP (Hypertext Transfer Protocol) is a protocol used for transmitting data over the internet, specifically for delivering web pages and other web-based content. A HTTP port is a network communication port that allows Hypertext Transfer Protocol (HTTP) traffic to be transmitted between a client and a server. The most commonly used HTTP port is 80.

An open HTTP port creates the possibility of an unencrypted connection being made between the server and a client. Any information passed across this unencrypted channel is vulnerable to a man-in-the-middle attack where sensitive information, including usernames and passwords, can be read in transit by a malicious third party.

All web traffic should be conducted over an HTTPS connection, typically using port 443. By proactively redirecting or blocking the unencrypted HTTP port, the risk of data interception is greatly reduced.

Expected	Ports > 'HTTP': [closed]
Actual	'HTTP': [listening on ports 2052, 2053, 2082, 2086, 2095, 2096, 8073, 8080, 8880]
First detected	Sep 11, 2025

'HTTPS' port open



141.193.213.20
141.193.213.21

HTTPS (HyperText Transfer Protocol Secure) is a secure protocol that is used to communicate over the internet. This protocol uses encryption to secure the data being transmitted between the server and client, preventing eavesdropping and tampering of the data. The most common port numbers used for HTTPS are 443, 80, and 8443.

Although HTTPS traffic is encrypted, web ports should only be enabled on servers intended to fill that role. For example, a database server should not have an open web port, especially to the internet. Arbitrarily open web ports increase the attack surface and could provide an inroad for an attacker to gain access to the system's true function.

Verify that the only servers with internet facing HTTPS ports are those intended to serve public webpages. Internal websites, web management tools and other sensitive web sites should be accessible to remote users via a VPN connection.

Expected	Ports > 'HTTPS': [closed]
Actual	'HTTPS': [listening on ports 2083, 2087, 6443, 8443]
First detected	May 28, 2025

Artificial Intelligence (AI) system usage detected



velocityrecoveries.com

Usage of AI systems can pose data security vulnerabilities, show unpredictable behaviours and have biases in outputs if not managed appropriately.

Determine the potential risk to your organization by checking the extent of AI system usage and any security controls that are in place.

Ensure appropriate security controls and AI system usage standards are in place by requesting the vendor complete the UpGuard AI-Risk Essentials questionnaire.

Expected	Artificial Intelligence (AI) system usage: [none found]
Actual	accessiBe (https://accessibe.com)
First detected	Mar 29, 2026

Unmaintained page detected



velocityrecoveries.com:443
www.velocityrecoveries.com:443

The response from the page indicates that it is a default server page or otherwise not configured and maintained for use.

Unmaintained assets increase the size of the attack surface and are more likely not to be continuously monitored and updated. These additional points on the attack surface give attackers more potential areas to target.

Sites that are not used should be decommissioned to reduce the attack surface. If the domain is hosting pages that are in use on some other URL and the index of the domain is not intended for the public, access should be removed.

Expected	Unmaintained Page: [not detected]
Actual	Status Code: 504, TLS handshake completed, no HTTP response
First detected	May 15, 2026

Certificate not found on our revoked certificate list



velocityrecoveries.com:2083
velocityrecoveries.com:2087
velocityrecoveries.com:443
velocityrecoveries.com:6443
velocityrecoveries.com:8443
www.velocityrecoveries.com:443

The site's certificate chain was checked against our list of revoked certificates.

Expected	SSL > Revoked: false
----------	----------------------

Actual	false
--------	-------

No unregistered MX records detected



velocityrecoveries.com

No unregistered MX records that could lead to receiving mail on behalf of the target organization were detected.

Expected	Unregistered MX Domains: [none]
----------	---------------------------------

Actual	[none]
--------	--------

Domain has not expired



velocityrecoveries.com

Domain has not expired.

Expected	Domain > Expired: [has not expired]
----------	-------------------------------------

Actual	2028-07-25T18:37:03.000Z
--------	--------------------------

No subdomain takeover vulnerability detected



velocityrecoveries.com:2052
velocityrecoveries.com:2053
velocityrecoveries.com:2082
velocityrecoveries.com:2083
velocityrecoveries.com:2086
velocityrecoveries.com:2087
velocityrecoveries.com:2095
velocityrecoveries.com:2096
velocityrecoveries.com:443
velocityrecoveries.com:6443
velocityrecoveries.com:8073
velocityrecoveries.com:8080
velocityrecoveries.com:8443
velocityrecoveries.com:8880
www.velocityrecoveries.com:2052
www.velocityrecoveries.com:2053

No dangling DNS records that could lead to subdomain takeover were detected.

Expected	Subdomain Takeover: [not vulnerable]
----------	--------------------------------------

Actual	[not vulnerable]
--------	------------------

DMARC policy exists



velocityrecoveries.com

DMARC protects against fraudulent emails being sent from a domain.

Expected	DNS > DMARC: v=DMARC1; p=reject; ...
----------	--------------------------------------

Actual	v=DMARC1;p=quarantine;sp=quarantine;pct=100;adkim=r;aspf=r;rua=mailto:tech@velocityrecoveries.com;ruf=mailto:tech@velocityrecoveries.com;fo=1
--------	---

Strict SPF filtering - not using +all
velocityrecoveries.com



Sender Policy Framework (SPF) record strictly enforces specific domains allowed to send email on its behalf.

Expected DNS > SPF > Filter: contains -all

Actual contains -all

SSL has not expired



velocityrecoveries.com:2083
velocityrecoveries.com:2087
velocityrecoveries.com:443
velocityrecoveries.com:6443
velocityrecoveries.com:8443
www.velocityrecoveries.com:443

SSL certificate has not expired.

Expected SSL > Expired: [has not expired]

Actual 2026-07-04 17:12:49 UTC, 2026-05-22 06:54:13 UTC, 2026-07-05 18:04:24 UTC

Trusted SSL certificate



velocityrecoveries.com:2083
velocityrecoveries.com:2087
velocityrecoveries.com:443
velocityrecoveries.com:8443
www.velocityrecoveries.com:443

The certificate presented by this domain was issued by a trusted certificate authority.

Expected SSL > Trusted: true

Actual true

Not a suspected malware provider



velocityrecoveries.com

This website does not appear to contain malicious code.

Expected Google Safe Browsing > Malware: false

Actual false

No reports of botnet activity in the last 30 days



This IP/domain has not been reported as a source of botnet activity in the last 30 days.

Expected Botnet Activity: false

Actual

No reports of brute force login attempts in the last 30 days



This IP/domain did not appear on any list of IPs and domains known to perform brute force login attempts in the last 30 days.

Expected Unsolicited Communication > Brute Force Login Attempt: false

Actual

No reports of malware distribution in the last 30 days



This IP/domain has been reported for distributing malware in the last 30 days.

Expected Malware Server: false

Actual

No reports of unsolicited scanning in the last 30 days



This IP/domain has not been reported for performing unsolicited scanning in the last 30 days.

Expected Unsolicited Communication > Scanning: false

Actual

Not suspected of unwanted software



velocityrecoveries.com

This website does not appear to be attempting to install unwanted software.

Expected Google Safe Browsing > Unwanted Software: false

Actual false

Not a suspected phishing page



velocityrecoveries.com

This site does not appear to be a forgery or imitation of another website.

Expected Google Safe Browsing > Phishing: false

Actual false

No reports of phishing activity in the last 30 days



This IP/domain has not been reported as a phishing site in the last 30 days.

Expected Phishing Site: false

Actual

No listable directories found



velocityrecoveries.com

No listable directories were found on the server.

Expected Listable Directories: [none]

Actual [none]

Domain does not expire soon



velocityrecoveries.com

Domain does not expire within 30 days.

Expected Domain > Expires On: [does not expire in next 30 days]

Actual 2028-07-25T18:37:03.000Z

SPF syntax correct



velocityrecoveries.com

Sender Policy Framework (SPF) record passes basic syntax checks.

Expected DNS > SPF > Syntax: passes simple syntax check

Actual passes simple syntax check

No insecure SSL/TLS versions available



No insecure SSL/TLS versions are available for this site.

Expected SSL > Insecure Protocol Versions: [none found]

Actual [none found]

SSL certificate chain present in server response



velocityrecoveries.com:2083
velocityrecoveries.com:2087
velocityrecoveries.com:443
velocityrecoveries.com:8443
www.velocityrecoveries.com:443

A complete SSL certificate chain was presented by the server for this domain.

Expected	SSL > Chain: [certificate chain present in server response]
Actual	present

SSL chain certificates do not expire within 20 days



velocityrecoveries.com:2083
velocityrecoveries.com:2087
velocityrecoveries.com:443
velocityrecoveries.com:8443
www.velocityrecoveries.com:443

SSL intermediate and root certificates do not expire within 20 days.

Expected	SSL > Chain: [does not expire within 20 days]
Actual	[none found]

SSL expiration period shorter than 398 days



velocityrecoveries.com:2083
velocityrecoveries.com:2087
velocityrecoveries.com:443
velocityrecoveries.com:6443
velocityrecoveries.com:8443
www.velocityrecoveries.com:443

The SSL certificate presented by the server has an expiration period shorter than 398 days.

Expected	SSL > Expires: [expiration period shorter than 398 days]
Actual	90, 30

SSL has more than 20% of its valid period remaining



velocityrecoveries.com:2083
velocityrecoveries.com:2087
velocityrecoveries.com:443
velocityrecoveries.com:6443
velocityrecoveries.com:8443
www.velocityrecoveries.com:443

SSL certificate does not expire in less than 20% of its total valid period.

Expected	SSL > Expires: [has more than 20% of its valid period remaining]
Actual	2026-07-04 17:12:49 UTC, 2026-05-22 06:54:13 UTC, 2026-07-05 18:04:24 UTC

Strong SSL algorithm



velocityrecoveries.com:2083
velocityrecoveries.com:2087
velocityrecoveries.com:443
velocityrecoveries.com:6443
velocityrecoveries.com:8443
www.velocityrecoveries.com:443

Industry standard SHA-256 encryption in use.

Expected	SSL > Algorithm: [at least 'sha256']
Actual	ECDSA-SHA256



Not vulnerable to CVE-2014-0160 (Heartbleed)

A bug in OpenSSL's implementation of the TLS heartbeat extension allows access to portions of memory on the targeted host e.g. cryptographic keys and passwords.

Expected Vulnerabilities > CVE-2014-0160: [not vulnerable]

Actual [not vulnerable]

Not vulnerable to CVE-2014-3566 (POODLE)

The server does not support SSLv3, and is not vulnerable to the POODLE attack.

Expected Vulnerabilities > CVE-2014-3566: [not vulnerable]

Actual [not vulnerable]

Not vulnerable to CVE-2015-0204 (FREAK)

The server does not offer RSA_EXPORT cipher suites, so clients are not vulnerable to the FREAK attack.

Expected Vulnerabilities > CVE-2015-0204: [not vulnerable]

Actual [not vulnerable]

Not vulnerable to CVE-2015-4000 (Logjam)

The server is using strong Diffie-Hellman parameters and is not vulnerable to the Logjam attack.

Expected Vulnerabilities > CVE-2015-4000: [not vulnerable]

Actual [not vulnerable]

Secure cookies used

velocityrecoveries.com:2052
velocityrecoveries.com:2082
velocityrecoveries.com:2083
velocityrecoveries.com:2086
velocityrecoveries.com:2087
velocityrecoveries.com:2095
velocityrecoveries.com:8080
velocityrecoveries.com:8443
velocityrecoveries.com:8880
www.velocityrecoveries.com:2052

Using secure cookies reduces the risk of third parties intercepting information contained in these cookies.

Expected Headers: [all set-cookie headers include 'secure']

Actual [no set-cookie headers]

Server information header not exposed

velocityrecoveries.com:2052
velocityrecoveries.com:2053
velocityrecoveries.com:2082
velocityrecoveries.com:2083
velocityrecoveries.com:2086
velocityrecoveries.com:2087
velocityrecoveries.com:2095
velocityrecoveries.com:2096
velocityrecoveries.com:443
velocityrecoveries.com:6443
velocityrecoveries.com:8073
velocityrecoveries.com:8080
velocityrecoveries.com:8443
velocityrecoveries.com:8880
www.velocityrecoveries.com:2052
www.velocityrecoveries.com:2053
www.velocityrecoveries.com:443

Ensuring the server information header is not exposed reduces the ability of attackers to exploit certain vulnerabilities.

Expected	Headers > server: [does not contain version number]
Actual	cloudflare, cloudflare-nginx

X-Powered-By header not exposed



velocityrecoveries.com:2052
velocityrecoveries.com:2053
velocityrecoveries.com:2082
velocityrecoveries.com:2083
velocityrecoveries.com:2086
velocityrecoveries.com:2087
velocityrecoveries.com:2095
velocityrecoveries.com:2096
velocityrecoveries.com:443
velocityrecoveries.com:6443
velocityrecoveries.com:8073
velocityrecoveries.com:8080
velocityrecoveries.com:8443
velocityrecoveries.com:8880
www.velocityrecoveries.com:2052
www.velocityrecoveries.com:2053
www.velocityrecoveries.com:443

Information about specific technology used on the server is obscured.

Expected	Headers > x-powered-by: [not set]
Actual	[not set]

X-Frame-Options is not deny or sameorigin



velocityrecoveries.com:443

Browsers are prevented from displaying this website's content in frames. This helps mitigate clickjacking attacks.

Expected	Headers > x-frame-options: [deny or sameorigin]
Actual	SAMEORIGIN

HttpOnly cookies used



velocityrecoveries.com:2052
velocityrecoveries.com:2082
velocityrecoveries.com:2083
velocityrecoveries.com:2086
velocityrecoveries.com:2087
velocityrecoveries.com:2095
velocityrecoveries.com:8080
velocityrecoveries.com:8443
velocityrecoveries.com:8880
www.velocityrecoveries.com:2052

Using HttpOnly cookies reduces the risk of client side script attacks, by preventing cookies being read on the client.

Expected	Headers: [all set-cookie headers include 'httponly']
Actual	[no set-cookie headers]

WordPress XML-RPC API disabled



velocityrecoveries.com

The WordPress XML-RPC API can provide an additional surface for DDoS and brute force attacks. It should be disabled when possible.

Expected	WordPress XML-RPC API enabled: false
Actual	false

WordPress version not exposed



velocityrecoveries.com

Ensuring the WordPress version is not exposed can make it harder for attackers to find exploits against your site.

Expected	WordPress Version: [not exposed]
Actual	[not exposed]

WordPress plugin versions not exposed

velocityrecoveries.com



Ensuring WordPress plugin versions are not exposed can make it harder for attackers to find exploits against your site.

Expected	WordPress Plugin Versions: [not exposed]
Actual	[not exposed]

WordPress user list not exposed

velocityrecoveries.com



Exposing the list of users on a WordPress site (via the WP-JSON API) can assist attackers in brute forcing credentials, as well as constitute a privacy risk.

Expected	WordPress Users: [none]
Actual	[none]

DNSSEC enabled

velocityrecoveries.com



DNSSEC records prevent third parties from forging the records that guarantee a domain's identity.

Expected	DNSSEC enabled: true
Actual	true

Domain not flagged as inactive

velocityrecoveries.com



Domain is not flagged as inactive.

Expected	Domain > Not Resolvable: inactive: not set
Actual	inactive: not set

Domain not pending deletion

velocityrecoveries.com



Domain is not pending deletion with the registrar.

Expected	Domain > Pending Deletion: pendingDelete: not set
Actual	pendingDelete: not set

Domain not pending restoration

velocityrecoveries.com



Domain is not pending restoration with the registrar.

Expected	Domain > Pending Restoration: pendingRestore: not set
Actual	pendingRestore: not set

Domain registrar or registry deletion protection enabled

velocityrecoveries.com



Domain is protected from unsolicited deletion requests with the registrar or registry.

Expected	Domain > Registrar Deletion Protection: clientDeleteProhibited or serverDeleteProhibited: set
----------	---

Expected	
Actual	clientDeleteProhibited:enabled

Domain registrar or registry transfer protection enabled
velocityrecoveries.com 

Domain is protected from unsolicited transfer requests.

Expected	Domain > Registrar Transfer Protection: clientTransferProhibited or serverTransferProhibited: set
Actual	clientTransferProhibited:enabled

Domain registrar or registry update protection enabled
velocityrecoveries.com 

Domain is protected from unsolicited update requests with the registrar or registry.

Expected	Domain > Registrar Update Protection: clientUpdateProhibited: set or serverUpdateProhibited: set
Actual	clientUpdateProhibited:enabled

Domain free of registrar DNS resolution hold
velocityrecoveries.com 

Domain is not under a DNS resolution hold with the registrar.

Expected	Domain > Registrar DNS Resolution Hold: clientHold: not set
Actual	clientHold: not set

Domain free of registry DNS resolution hold
velocityrecoveries.com 


Domain is not under a DNS resolution hold with the registry itself.

Expected	Domain > Registry DNS Resolution Hold: serverHold: not set
Actual	serverHold: not set

DMARC policy percentage is default
velocityrecoveries.com 

DMARC policy percentage is set to default 100%, ensuring all mail is covered by the policy.

Expected	DNS > DMARC: v=DMARC1; p=reject; pct=100...
Actual	v=DMARC1;p=quarantine;sp=quarantine;pct=100;adkim=r;aspf=r;rua=mailto:tech@velocityrecoveries.com;ruf=mailto:tech@velocityrecoveries.com;fo=1

SPF ptr mechanism not used
velocityrecoveries.com 

Sender Policy Framework (SPF) record does not include the ptr mechanism.

Expected	DNS > SPF > ptr: SPF record does not contain a ptr mechanism
Actual	SPF record does not contain a ptr mechanism

Strong public certificate key length 
 velocityrecoveries.com:2083
 velocityrecoveries.com:2087
 velocityrecoveries.com:443
 velocityrecoveries.com:6443
 velocityrecoveries.com:8443
 www.velocityrecoveries.com:443

The site's public certificate provides at least 112 bits of security strength.

Expected	SSL > Public Certificate Key Length: [RSA >= 2048 or ECDSA >= 224]
Actual	256-bit ECDSA

Referrer policy is not unsafe-url
velocityrecoveries.com:443



The website's Referrer Policy is not configured to allow unsafe information to be sent in the referrer header.

Expected	Headers > referrer-policy: [not unsafe-url]
Actual	same-origin

ASP.NET version header not exposing specific ASP.net version



velocityrecoveries.com:2052
velocityrecoveries.com:2053
velocityrecoveries.com:2082
velocityrecoveries.com:2083
velocityrecoveries.com:2086
velocityrecoveries.com:2087
velocityrecoveries.com:2095
velocityrecoveries.com:2096
velocityrecoveries.com:443
velocityrecoveries.com:6443
velocityrecoveries.com:8073
velocityrecoveries.com:8080
velocityrecoveries.com:8443
velocityrecoveries.com:8880
www.velocityrecoveries.com:2052
www.velocityrecoveries.com:2053
www.velocityrecoveries.com:443

Ensuring the ASP.NET version header is not exposing a specific version makes it harder for attackers to exploit certain vulnerabilities.

Expected	Headers > x-aspnet-version: [not set]
Actual	[not set]

ASP.NET version header not exposed



velocityrecoveries.com:2052
velocityrecoveries.com:2053
velocityrecoveries.com:2082
velocityrecoveries.com:2083
velocityrecoveries.com:2086
velocityrecoveries.com:2087
velocityrecoveries.com:2095
velocityrecoveries.com:2096
velocityrecoveries.com:443
velocityrecoveries.com:6443
velocityrecoveries.com:8073
velocityrecoveries.com:8080
velocityrecoveries.com:8443
velocityrecoveries.com:8880
www.velocityrecoveries.com:2052
www.velocityrecoveries.com:2053
www.velocityrecoveries.com:443

Ensuring the ASP.NET version header is not exposed makes it harder for attackers to exploit certain vulnerabilities.

Expected	Headers > x-aspnet-version present: [not present]
Actual	[not present]

No open cloud storage service detected



velocityrecoveries.com:2052
velocityrecoveries.com:2053
velocityrecoveries.com:2082

velocityrecoveries.com:2083
velocityrecoveries.com:2086
velocityrecoveries.com:2087
velocityrecoveries.com:2095
velocityrecoveries.com:2096
velocityrecoveries.com:443
velocityrecoveries.com:6443
velocityrecoveries.com:8073
velocityrecoveries.com:8080
velocityrecoveries.com:8443
velocityrecoveries.com:8880
www.velocityrecoveries.com:2052
www.velocityrecoveries.com:2053

No cloud storage service configured to allow anonymous file listing was detected.

Expected	Open Cloud Storage: [not detected]
Actual	[not detected]

Domain index is not a listable directory



velocityrecoveries.com:2052
velocityrecoveries.com:2053
velocityrecoveries.com:2082
velocityrecoveries.com:2083
velocityrecoveries.com:2086
velocityrecoveries.com:2087
velocityrecoveries.com:2095
velocityrecoveries.com:2096
velocityrecoveries.com:443
velocityrecoveries.com:6443
velocityrecoveries.com:8073
velocityrecoveries.com:8080
velocityrecoveries.com:8443
velocityrecoveries.com:8880
www.velocityrecoveries.com:2052
www.velocityrecoveries.com:2053

The domain index is not a listable directory.

Expected	Domain Index: [not a listable directory]
Actual	[not a listable directory]

Domain renewal not prohibited by registry



velocityrecoveries.com

Domain is not prohibited from renewal at the registry itself.

Expected	Domain > Prohibited from Renewal at Registry: serverRenewProhibited: not set
Actual	serverRenewProhibited: not set

No reports of botnet activity in the last 90 days



This IP/domain has not been reported as a source of botnet activity in the last 90 days.

Expected	Botnet Activity: false
Actual	

No reports of brute force login attempts in the last 90 days



This IP/domain did not appear on any list of IPs and domains known to perform brute force login attempts in the last 90 days.

Expected	Unsolicited Communication > Brute Force Login Attempt: false
Actual	

No reports of malware distribution in the last 90 days



This IP/domain has been reported for distributing malware in the last 90 days.

Expected	Malware Server: false
Actual	

No reports of unsolicited scanning in the last 90 days



This IP/domain has not been reported for performing unsolicited scanning in the last 90 days.

Expected	Unsolicited Communication > Scanning: false
Actual	

No reports of phishing activity in the last 90 days



This IP/domain has not been reported as a phishing site in the last 90 days.

Expected	Phishing Site: false
Actual	

Headquartered in a country with established political freedoms



The vendor is not known to operate primarily out of a jurisdiction classified as having low political freedom.

Expected	Operating in a country of low political freedom: false
Actual	false