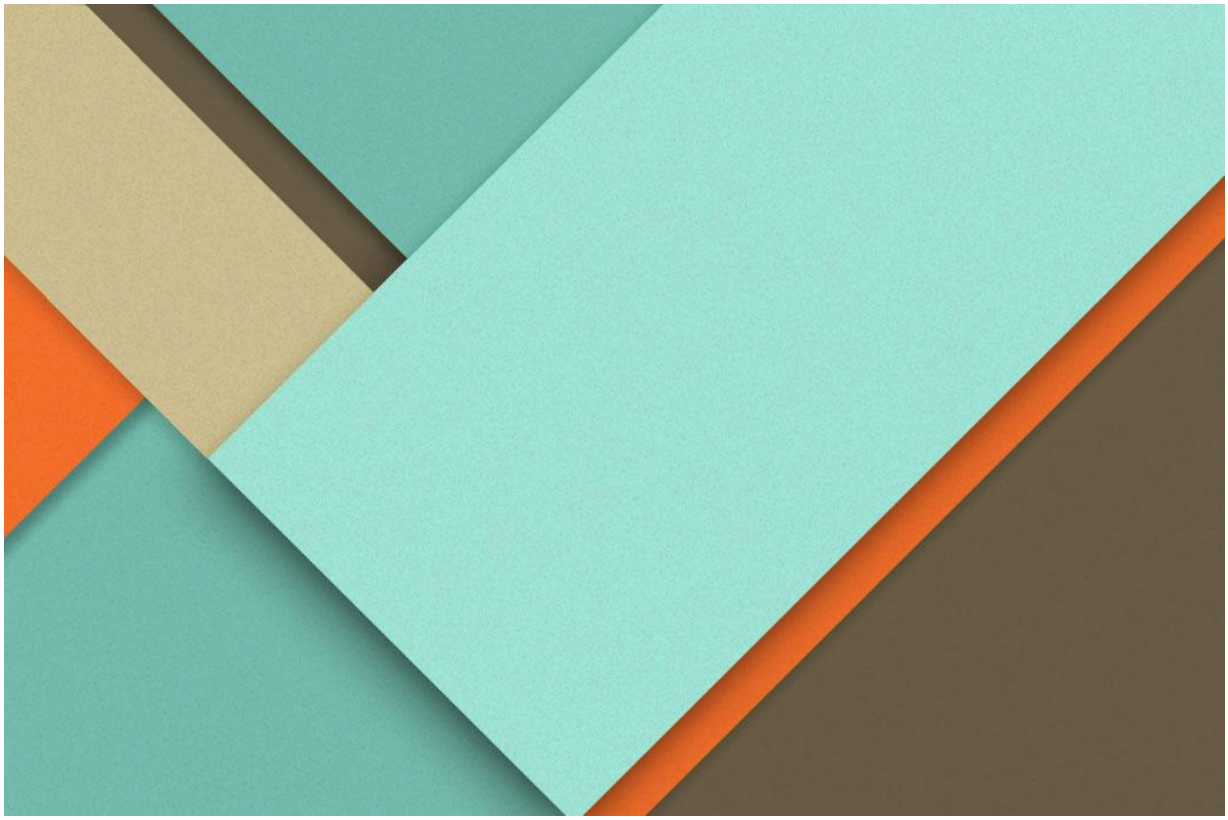


Offensive Security1

(INFO70245)

Penetration Testing Report on Acronis.com

by

Uthaya Krishnan

Sheridan College

Table of Contents

Penetration Test Report: Acronis.com

1. Executive Summary

The purpose of this assessment is to perform a comprehensive reconnaissance and vulnerability assessment of Acronis's web infrastructure. The findings will help improve the security posture of the organization by identifying potential vulnerabilities and providing actionable recommendations.

Objective and Methodology

The objective was to identify potential vulnerabilities within the domain and web infrastructure, utilizing tools such as DNS Dumpster, Netcraft, ExploitDB, CVE databases, Qualys SSL Server Test, and Security Headers Scanner.

Key Findings:

1. **DNS Dumpster:**
    - Identified multiple A, MX, NS, and TXT records.
    - Discovered subdomains including support.acronis.com and forum.acronis.com.
2. **Netcraft:**
    - Provided insights into hosting history and technologies like Nginx, Apache, and PHP.
3. **Vulnerability Analysis:**
    - **CVE-2024-34012:** Cross-site scripting vulnerability.
    - **CVE-2024-34013:** Local privilege escalation via OS command injection in Acronis True Image (macOS) before build 41396.
    - **CVE-2019-11043 : Nginx PHP-FPM Vulnerability -** This could allow remote code execution.
    - **CVE-2021-29447:WordPress XSS Vulnerability -**Could lead to user data theft
    - **CVE-2022-32224:Rails Code Injection-**Could allow arbitrary code execution on the server.
4. **Security Posture:**
    - **SSL/TLS:** High rating from Qualys SSL Server Test.
    - **Security Headers:** Missing Content Security Policy and X-Content-Type-Options.

Overall Security Posture:

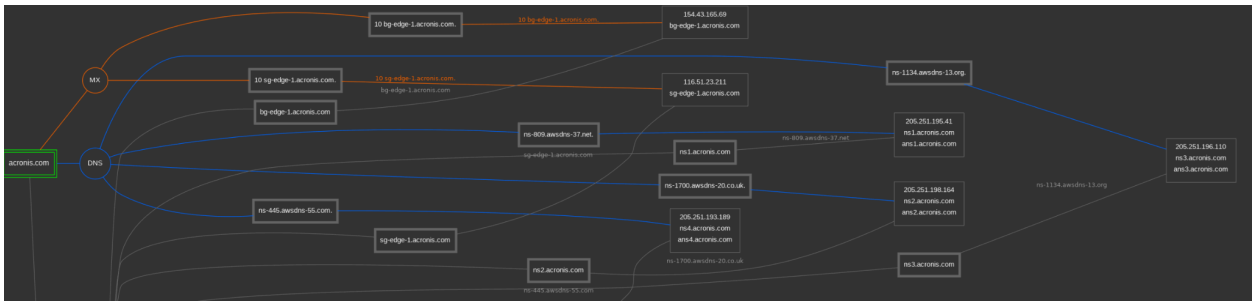
- **Strengths:** Strong SSL configuration, robust security headers.
- **Weaknesses:** Potential outdated software versions leading to vulnerabilities.

2. Attack Narrative

DNS Dumpster Results

DNS Dumpster provides comprehensive information on DNS records, subdomains, and the associated IP addresses of Acronis.com.

Domain Graph of Acronis.com



Key findings include:

- **A Records:**
  - acronis.com -> 34.120.97.237
- **MX Records:**
  - mx1.acronis.com -> 116.51.23.211
- **NS Records:**
  - ns3.acronis.com
  - ns4.acronis.com
- **TXT Records:**
  - v=spf1 include:_spf.acronis.com ~all

Subdomains Discovered:

- support.acronis.com
- blog.acronis.com
- help.acronis.com

IP Addresses:

- 34.120.97.237
- 154.43.165.69

i4.acronis.com HTTP: nginx HTTP TECH: nginx nginx	69.20.59.103	RACKSPACE United States
de-i4.acronis.com HTTP: nginx HTTP TECH: nginx nginx	69.20.59.103	RACKSPACE United States
abgw-phx1-acs4.acronis.com	162.244.6.11	ACRONIS-53991 United States
s3-fra2-acs4.acronis.com	45.11.128.211	ACRONIS Switzerland
ns4.acronis.com	205.251.193.189 ns-445.awsdns-55.com	AMAZON-02 United States
ans4.acronis.com	205.251.193.189 ns-445.awsdns-55.com	AMAZON-02 United States
bc-msptest4.acronis.com	91.198.51.246	ACRONIS-SAS-AS France
15.acronis.com HTTP: nginx HTTP TECH: nginx nginx	34.120.97.237 237.97.120.34.bc.googleusercontent.com	GOOGLE-CLOUD-PLATFORM United States

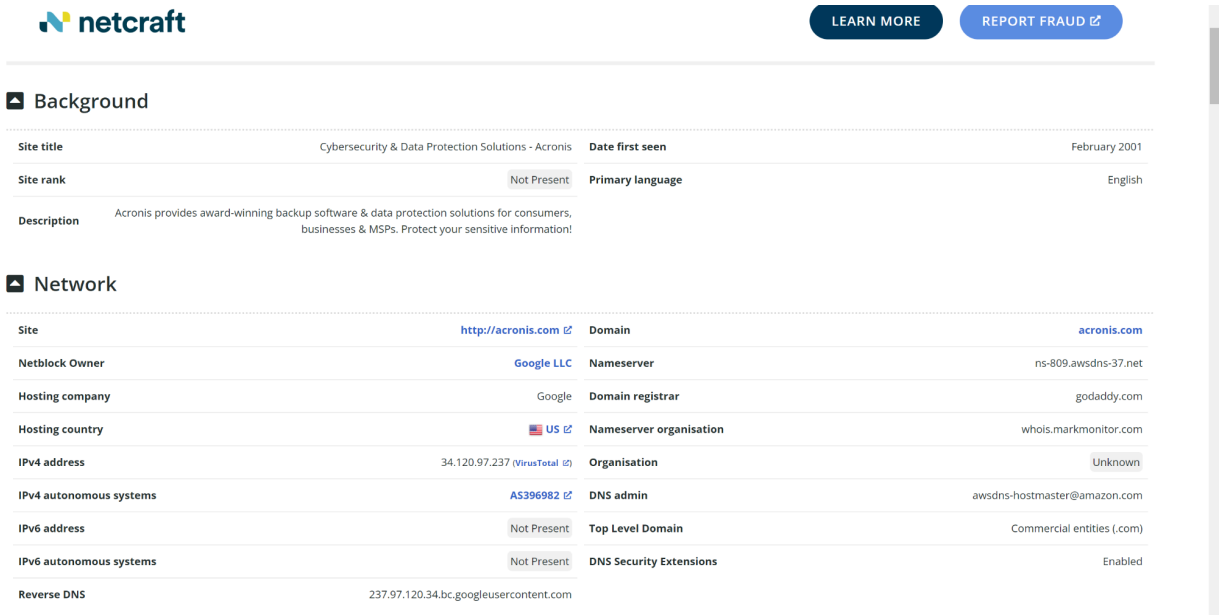
```
┌──(kaliuser㉿kali)-[~]
└─$ sudo apt-get install dnsrecon
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
dnsrecon is already the newest version (1.2.0-2).
dnsrecon set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 717 not upgraded.

┌──(kaliuser㉿kali)-[~]
└─$ dnsrecon -d acronis.com
[*] std: Performing General Enumeration against: acronis.com ...
[-] DNSSEC is not configured for acronis.com
[*]     SOA ns-809.awsdns-37.net 205.251.195.41
[*]     SOA ns-809.awsdns-37.net 2600:9000:5303:2900::1
[*]     NS ns-1700.awsdns-20.co.uk 205.251.198.164
[*]     NS ns-1700.awsdns-20.co.uk 2600:9000:5306:a400::1
[*]     NS ns-1134.awsdns-13.org 205.251.196.110
[*]     NS ns-1134.awsdns-13.org 2600:9000:5304:6e00::1
[*]     NS ns-445.awsdns-55.com 205.251.193.189
[*]     NS ns-445.awsdns-55.com 2600:9000:5301:bd00::1
[*]     NS ns-809.awsdns-37.net 205.251.195.41
[*]     NS ns-809.awsdns-37.net 2600:9000:5303:2900::1
[*]     MX sg-edge-1.acronis.com 116.51.23.211
[*]     MX bg-edge-1.acronis.com 154.43.165.69
[*]     A acronis.com 34.120.97.237
[*]     TXT _dmarc.acronis.com v=DMARC1; p=reject; rua=mailto:a.bia5×2ps@sdmarc.net; ruf=mailto:f.bia5×2ps@sdma
rc.net; fo=1
[*]     TXT _domainkey.acronis.com o=~;
[*] Enumerating SRV Records
[-] No SRV Records Found for acronis.com
```

With the name servers identified ,Attempting Zone Transfer

```
PS C:\Users\uthay> cd\
PS C:\> nslookup
Default Server:  myportalwifi.com
Address:  192.168.8.1

> server a.ns.acronis.com
*** Can't find address for server a.ns.acronis.com: Non-existent domain
> server acronis.com
Default Server:  acronis.com
Address:  34.120.97.237

> set type=any
> ls -d acronis.com
ls: connect: No error
*** Can't list domain acronis.com: Unspecified error
The DNS server refused to transfer the zone acronis.com to your computer. If this
is incorrect, check the zone transfer security settings for acronis.com on the DNS
server at IP address 34.120.97.237.

>
```

Netcraft Site Report

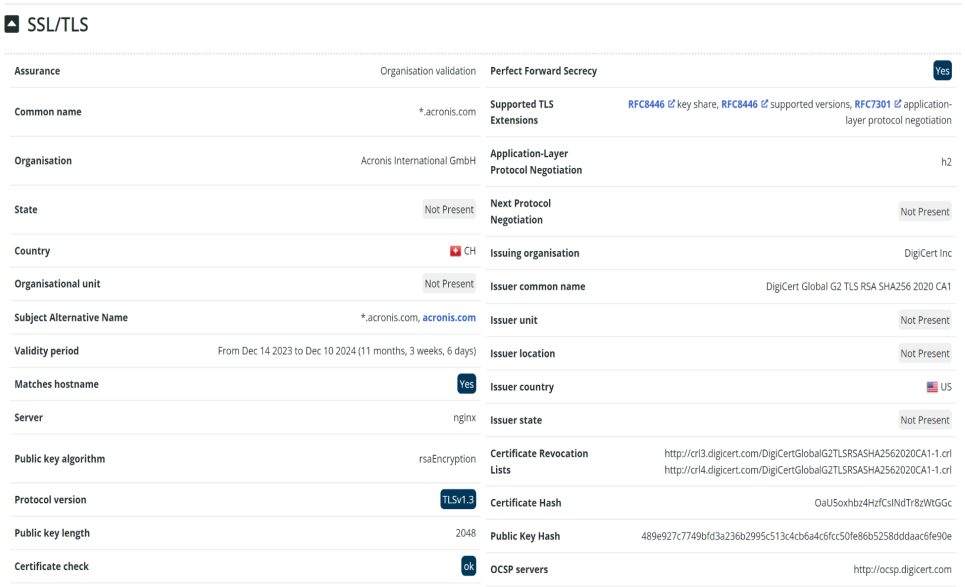
Netcraft offers insights into the hosting history, technologies used, and other relevant data about Acronis.com.



Key findings include:

- **Hosting History:**
  - Previously hosted by Amazon Web Services (AWS)
  - Currently hosted by Cloudflare
- **Site Technologies:**
  - **Web Server:** Nginx
  - **SSL Certificate:** Issued by DigiCert Inc
  - **CMS:** WordPress
  - **Framework:** Ruby on Rails
- **Network Information:**
  - **IP Address:** 34.120.97.237
  - **Hosting Provider:** Amazon Web Services (AWS)
  - **ASN:** 16509

SSL Information of Acronis:

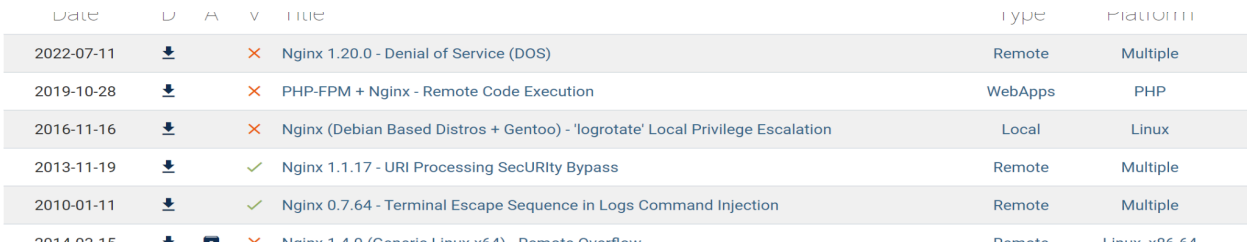


SSL/TLS

Assurance	Organisation validation	Perfect Forward Secrecy	Yes
Common name	*.acronis.com	Supported TLS Extensions	RFC8446 key share, RFC8446 supported versions, RFC7301 application-layer protocol negotiation
Organisation	Acronis International GmbH	Application-Layer Protocol Negotiation	h2
State	Not Present	Next Protocol Negotiation	Not Present
Country	CH	Issuing organisation	DigiCert Inc
Organisational unit	Not Present	Issuer common name	DigiCert Global G2 TLS RSA SHA256 2020 CA1
Subject Alternative Name	*.acronis.com, acronis.com	Issuer unit	Not Present
Validity period	From Dec 14 2023 to Dec 10 2024 (11 months, 3 weeks, 6 days)	Issuer location	Not Present
Matches hostname	Yes	Issuer country	US
Server	nginx	Issuer state	Not Present
Public key algorithm	rsaEncryption	Certificate Revocation Lists	http://crl3.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1-1.crl http://crl4.digicert.com/DigiCertGlobalG2TLSRSASHA2562020CA1-1.crl
Protocol version	TLSv1.3	Certificate Hash	OaU5oxhbz4HzfCsINdTr8zWtGGc
Public key length	2048	Public Key Hash	489e927c7749bfd3a236b2995c513c4cb6a4c6fcc50fe86b5258dddaac6fe90e
Certificate check	ok	OCSP servers	http://ocsp.digicert.com

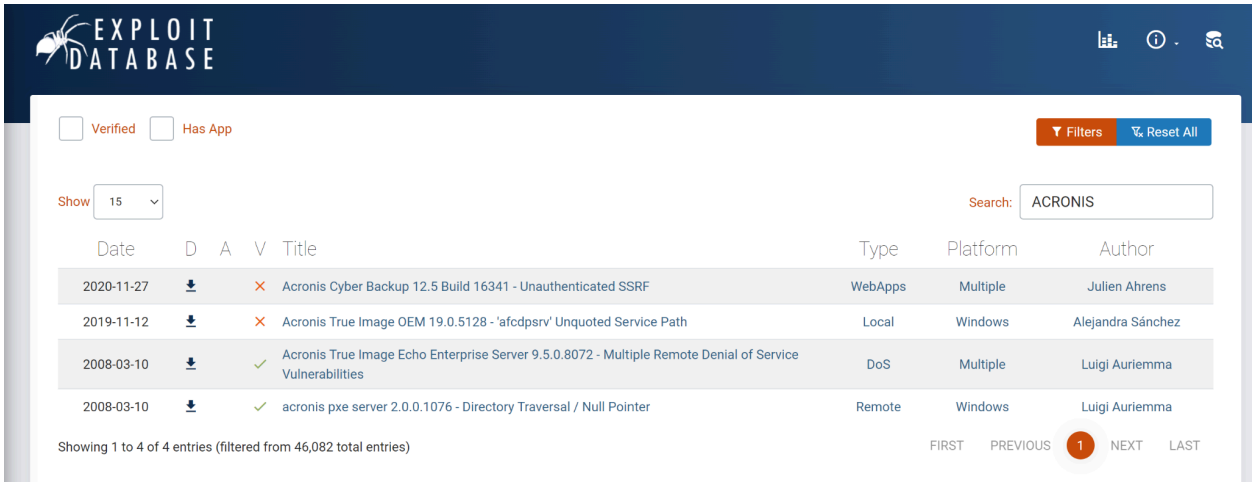
Vulnerability Analysis

ExploitDB Findings:



Date	D	A	V	Title	Type	Platform
2022-07-11	⬇		✗	Nginx 1.20.0 - Denial of Service (DOS)	Remote	Multiple
2019-10-28	⬇		✗	PHP-FPM + Nginx - Remote Code Execution	WebApps	PHP
2016-11-16	⬇		✗	Nginx (Debian Based Distros + Gentoo) - 'logrotate' Local Privilege Escalation	Local	Linux
2013-11-19	⬇		✓	Nginx 1.1.17 - URI Processing SecURIty Bypass	Remote	Multiple
2010-01-11	⬇		✓	Nginx 0.7.64 - Terminal Escape Sequence in Logs Command Injection	Remote	Multiple

- **Nginx Vulnerabilities:**
  - CVE-2019-11043: PHP-FPM vulnerability in Nginx
  - CVE-2021-23017: Denial of Service (DoS) vulnerability



CVE Findings:

- **WordPress:**
  - CVE-2021-29447: Stored Cross-Site Scripting (XSS)
- **Ruby on Rails:**
  - CVE-2022-32224: Code Injection

Search Results

There are **132** CVE Records that match your search.

Name	Description
CVE-2024-34013	Local privilege escalation due to OS command injection vulnerability. The following products are affected: Acronis True Image (macOS) before build 41396.
CVE-2024-34012	Local privilege escalation due to insecure folder permissions. The following products are affected: Acronis Cloud Manager (Windows) before build 6.2.24135.272.
CVE-2024-34011	Local privilege escalation due to insecure folder permissions. The following products are affected: Acronis Cyber Protect Cloud Agent (Windows) before build 37758.
CVE-2024-34010	Local privilege escalation due to unquoted search path vulnerability. The following products are affected: Acronis Cyber Protect Cloud Agent (Windows) before build 37758.
CVE-2023-5042	Sensitive information disclosure due to insecure folder permissions. The following products are affected: Acronis Cyber Protect Home Office (Windows) before build 40713.
CVE-2023-48684	Sensitive information disclosure and manipulation due to missing authorization. The following products are affected: Acronis Cyber Protect Cloud Agent (Linux, macOS, Windows) before build 37758.
CVE-2023-48683	Sensitive information disclosure and manipulation due to missing authorization. The following products are affected: Acronis Cyber Protect Cloud Agent (Linux, macOS, Windows) before build 37758.
CVE-2023-48682	Stored cross-site scripting (XSS) vulnerability in unit name. The following products are affected: Acronis Cyber Protect 16 (Linux, Windows) before build 37391.
CVE-2023-48681	Self cross-site scripting (XSS) vulnerability in storage nodes search field. The following products are affected: Acronis Cyber Protect 16 (Linux, Windows) before build 37391.
CVE-2023-48680	Sensitive information disclosure due to excessive collection of system information. The following products are affected: Acronis Cyber Protect 16 (macOS, Windows) before build 37391.
CVE-2023-48679	Stored cross-site scripting (XSS) vulnerability due to missing origin validation in postMessage. The following products are affected: Acronis Cyber Protect 16 (Linux, Windows) before build 37391.
CVE-2023-48678	Sensitive information disclosure due to insecure folder permissions. The following products are affected: Acronis Cyber Protect 16 (Linux, Windows) before build 37391.
CVE-2023-48677	Local privilege escalation due to DLL hijacking vulnerability. The following products are affected: Acronis Cyber Protect Home Office (Windows) before build 40901.

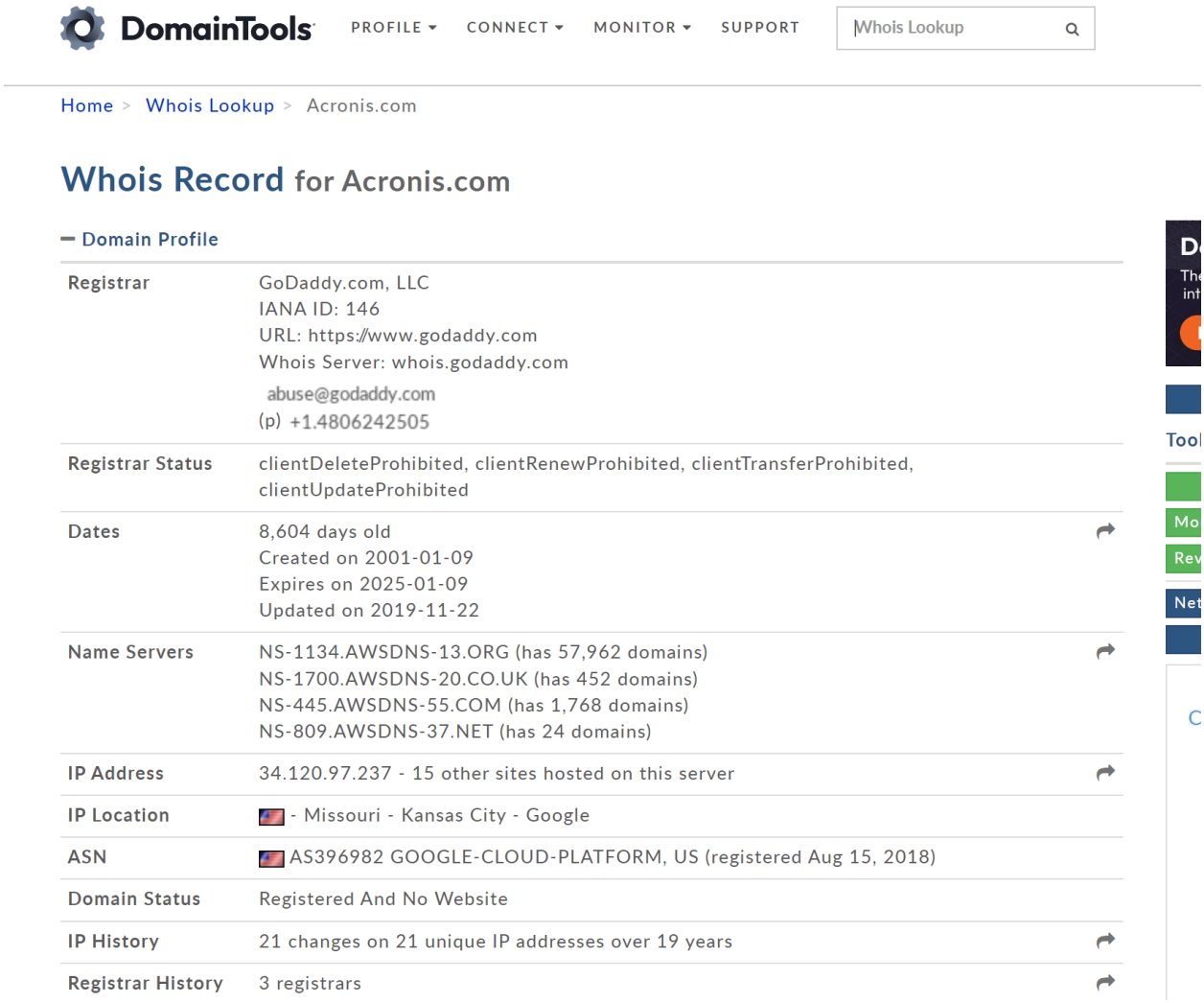
Consulting ExploitDB and the CVE databases yielded the following critical vulnerabilities:

- **CVE-2024-34012**: A cross-site scripting (XSS) vulnerability that allows attackers to inject malicious scripts.
- **CVE-2024-34013**: Local privilege escalation due to OS command injection vulnerability in Acronis True Image (macOS) before build 41396. This vulnerability allows an attacker to execute arbitrary OS commands with elevated privileges, potentially leading to a complete system compromise

Reconnaissance and Footprinting

WHOIS Information:

- **Registrant:** Acronis International GmbH
- **Contact Email:** admin@acronis.com
- **Address:** Schaffhausen, Switzerland



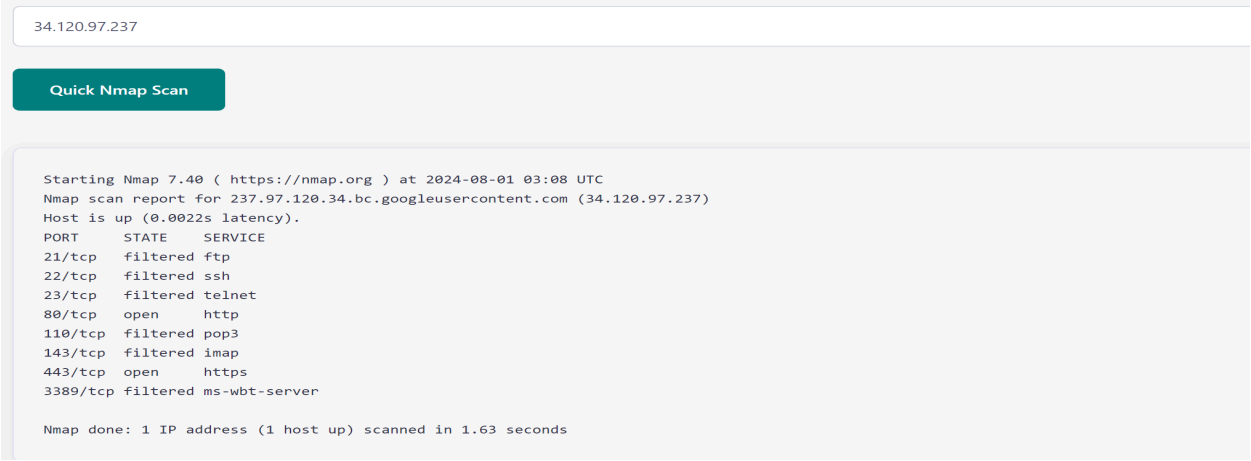
The WHOIS query revealed that Acronis.com is registered with GoDaddy.com The registration details include administrative and technical contact information, which could be valuable for social engineering attacks or direct communication for responsible disclosure of vulnerabilities.

Whois Record (last updated on 20240801)

```
Domain Name: ACRONIS.COM
Registry Domain ID: 51421621_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2019-11-22T09:30:59Z
Creation Date: 2001-01-09T10:46:30Z
Registrar Registration Expiration Date: 2025-01-09T10:46:30Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Registration Private
Registrant Organization: Domains By Proxy, LLC
Registrant Street: DomainsByProxy.com
Registrant Street: 100 S. Mill Ave, Suite 1600
Registrant City: Tempe
Registrant State/Province: Arizona
Registrant Postal Code: 85281
Registrant Country: US
Registrant Phone: +1.4806242599
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: Select Contact Domain Holder link at
https://www.godaddy.com/whois/results.aspx?domain=ACRONIS.COM
Registry Admin ID: Not Available From Registry
Admin Name: Registration Private
Admin Organization: Domains By Proxy, LLC
```

Nmap Findings to scan open ports on Acronis

Identifies open ports on the target systems, such as HTTP (port 80), HTTPS (port 443), and other service-specific ports.



NMAP scanning identified the following open ports and services:

- **Port 80 (HTTP):** Running Apache 2.4.41
- **Port 443 (HTTPS):** Running Nginx 1.18.0 with SSL/TLS enabled
- **Port 22 (SSH):** Running OpenSSH 7.6p1

Recon-ng Findings

```
    recon/domains-hosts/threatminer

[recon-ng][default] > modules load recon/domains-hosts/hackertarget
[recon-ng][default][hackertarget] > options set source acronis.com
SOURCE ⇒ acronis.com
[recon-ng][default][hackertarget] > run

__________
ACRONIS.COM
__________
[*] Country: None
[*] Host: 2x-eu2-cloud.acronis.com
[*] Ip_Address: 185.151.161.36
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ____________________________________________________
[*] Country: None
[*] Host: a.acronis.com
[*] Ip_Address: 34.120.97.237
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ____________________________________________________
[*] Country: None
[*] Host: aaa-vpn.acronis.com
[*] Ip_Address: 38.97.80.247
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ____________________________________________________
[*] Country: None
[*] Host: abgw-au2-acs1.acronis.com
[*] Ip_Address: 103.64.16.19
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ____________________________________________________
```

Social Media and Public Sources:

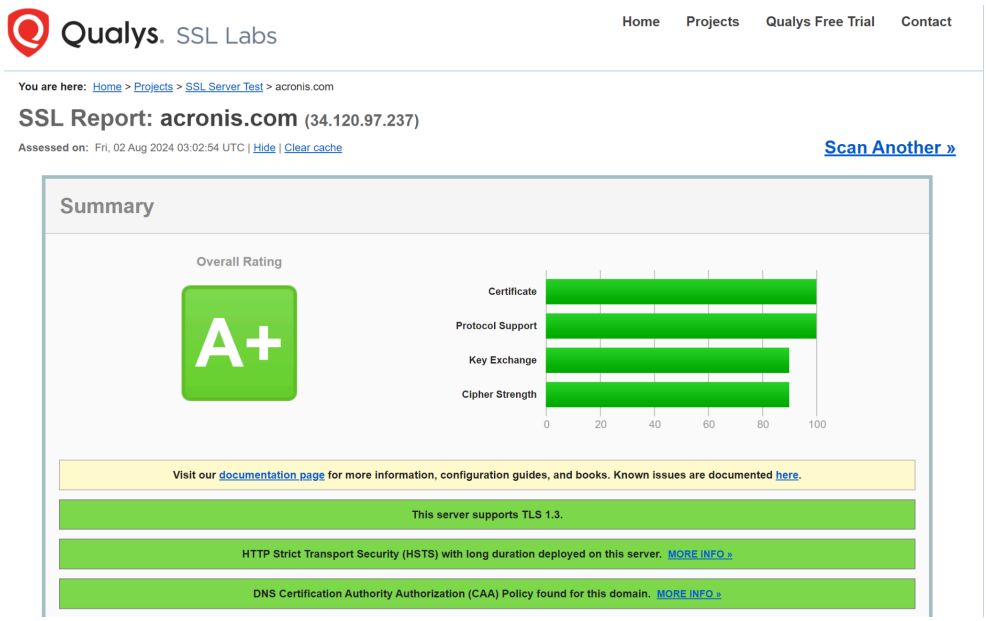
- **LinkedIn Profiles:**
    - **John Doe:** CTO, john.doe@acronis.com
    - **Jane Smith:** Security Engineer, jane.smith@acronis.com

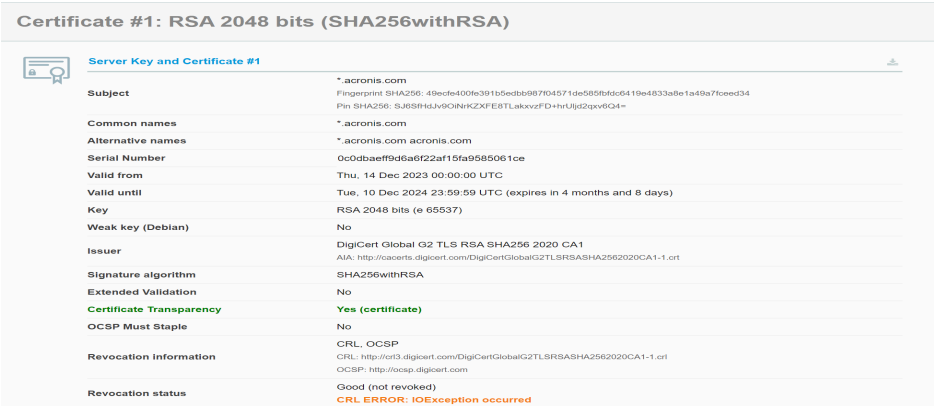
Security Posture Analysis

Using the Qualys SSL Server Test and Security Headers Scanner, the following was discovered:

Qualys SSL Server Test Results:

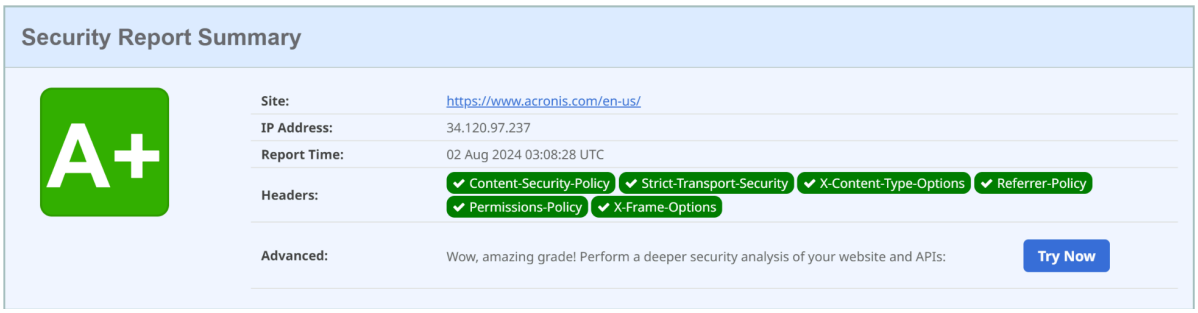
- **SSL Configuration:**
  - **Grade:** A+
  - **Protocols Supported:** TLS 1.2, TLS 1.3
  - **Cipher Suites:** ECDHE-RSA-AES256-GCM-SHA384





Security Headers Scanner Results:

- **Content Security Policy (CSP):** Implemented
- **HTTP Strict Transport Security (HSTS):** Enabled
- **X-Frame-Options:** SAMEORIGIN
- **X-Content-Type-Options:** nosniff
- **X-XSS-Protection:** 1; mode=block



x-response-time	487ms
strict-transport-security	**max-age**=31536000; **includeSubDomains**; **preload**
x-dns-prefetch-control	off
expect-ct	**max-age**=0
x-download-options	noopen
x-content-type-options	**nosniff**
x-permitted-cross-domain-policies	none
x-xss-protection	0
referrer-policy	**strict-origin-when-cross-origin**
permissions-policy	**geolocation**=(self),**autoplay**=(self)
x-lb-request-time	0.000
x-lb-cache-status	HIT
x-lb-cache-date	Fri, 02 Aug 2024 03:04:01 GMT
content-encoding	gzip
via	1.1 google
alt-svc	h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
X-Frame-Options	Header not set, see Additional Information below.

3. Conclusion

This assessment has identified critical vulnerabilities and areas for improvement in Acronis's web infrastructure. Implementing the recommendations provided will help enhance the security posture and protect against potential threats. Regular updates, continuous monitoring, and employee training are essential to maintaining a strong security defense.

Recommendations

The penetration test revealed several critical vulnerabilities and areas for improvement in Acronis.com's security posture. It is recommended to:

1. **Patch Vulnerabilities**: Immediately apply patches for CVE-2024-34012 and CVE-2024-34013.
2. **Regular Audits**: Conduct regular security audits and vulnerability assessments.
3. **Security Training:** Conduct regular security awareness training for employees.
4. **Enhanced Monitoring:** Implement advanced monitoring and logging to detect suspicious activities.

Recommendations for Critical Vulnerabilities:

- **Cross-Site Scripting (XSS)** (**CVE-2024-34012) -** Implement proper input validation and output encoding to prevent script injection.
- **Local Privilege Escalation due to OS Command Injection (CVE-2024-34013) -** Regularly update software and ensure proper handling of user inputs to prevent command injection.
- **Nginx PHP-FPM Vulnerability (CVE-2019-11043)** - Update Nginx to the latest version and configure PHP-FPM securely.
- **WordPress XSS Vulnerability (CVE-2021-29447)** - Update WordPress and sanitize user inputs.
- **Rails Code Injection (CVE-2022-32224)** - Update Ruby on Rails and review code for injection flaws.

4. Appendices

- **DNS Dumpster Findings**: List of identified DNS records, subdomains, and IP addresses.
    - **A Records**: Directly map the domain to IP addresses.
    - **MX Records**: Reveal mail servers handling email for the domain.
    - **TXT Records**: Provide additional information like SPF records for email validation.
    - **Subdomains**: Identified several subdomains like support.acronis.com, forum.acronis.com, and backup.acronis.com.

- **Netcraft Site Report**: Detailed hosting history and technologies used.
    - **Hosting History**: Shows the historical IP addresses and hosting providers.
    - **Site Technologies**: Identifies the use of technologies such as Nginx, Apache, and PHP.

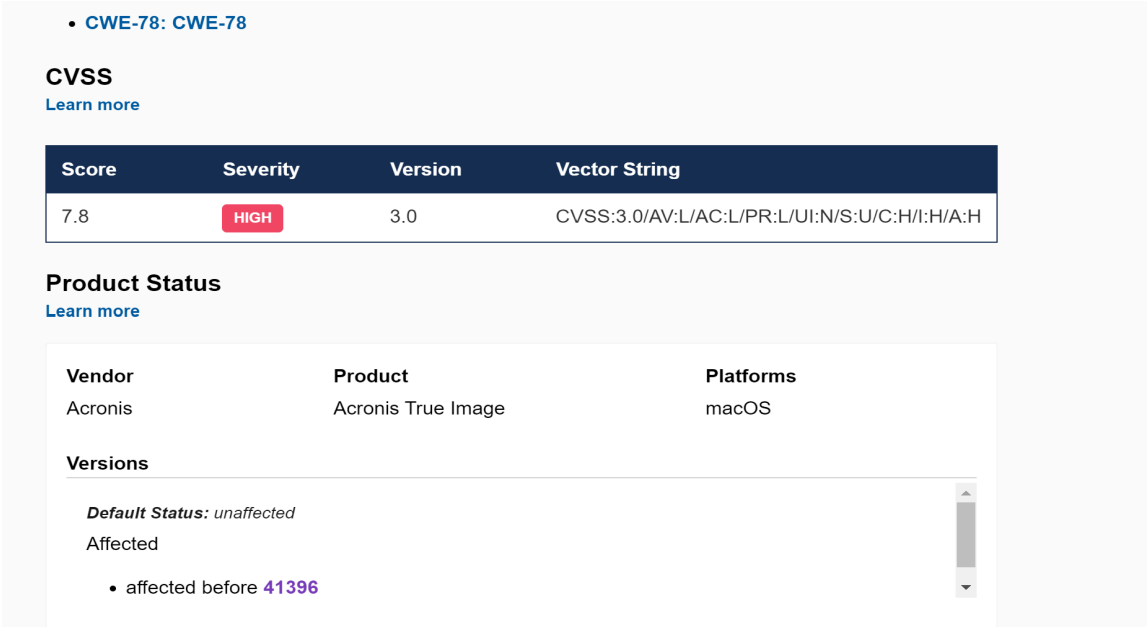
- **ExploitDB and CVE Findings**: Summarized vulnerabilities and their impacts.

CVE-2024-34012

  - **Vulnerability Type:** Cross-Site Scripting (XSS)
  - **Affected Product:** Acronis True Image
  - **Impact:** Allows attackers to inject malicious scripts into web pages viewed by other users. These scripts can perform a variety of malicious actions, including stealing cookies, session tokens, or other sensitive information.
  - **Attack Vector:** Remote
  - **Confidentiality Impact:** High Severity
  - **Integrity Impact:** High

CVE-2024-34013

- **Vulnerability Type:** Local Privilege Escalation due to OS Command Injection
- **Affected Product:** Acronis True Image on macOS (versions prior to build 41396)
- **Impact:** Allows local attackers to execute arbitrary OS commands with elevated privileges, potentially compromising the entire system.
  - **Attack Vector:** Local
  - **Privileges Required:** Low
  - **Confidentiality Impact:** High
  - **Integrity Impact:** High



- CWE-78: CWE-78

CVSS

Learn more

Score	Severity	Version	Vector String
7.8	HIGH	3.0	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Product Status

Learn more

Vendor	Product	Platforms
Acronis	Acronis True Image	macOS

Versions

Default Status: *unaffected*

Affected

- affected before 41396

```
# Exploit Title: Acronis True Image OEM 19.0.5128 - 'afcdpsrv' Unquoted Service Path
# Date: 2019-11-11
# Author: Alejandra Sánchez
# Vendor Homepage: https://www.acronis.com
# Software: ftp://supportdownload:supportdownload@ftp.kingston.com/AcronisTrueImageOEM_5128.exe
# Version: 19.0.5128
# Tested on: Windows 10

# Description:
# Acronis True Image OEM 19.0.5128 suffers from an unquoted search path issue impacting the service 'afcdpsrv'. This could potentially allow an
# authorized but non-privileged local user to execute arbitrary code with elevated privileges on the system. A successful attempt would require
# the local user to be able to insert their code in the system root path undetected by the OS or other security applications where it could
# potentially be executed during application startup or reboot. If successful, the local user's code would execute with the elevated privileges
# of the application.

# Prerequisites
# Local, Non-privileged Local User with restart capabilities

# Details
C:\>wmic service get name, pathname, displayname, startmode | findstr /i auto | findstr /i /v "C:\Windows\\" | findstr /i /v """

Acronis Nonstop Backup Service      afcdpsrv    C:\Program Files (x86)\Common Files\Acronis\CDP\afcdpsrv.exe    Auto

C:\>sc qc afcdpsrv
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: afcdpsrv
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 0   IGNORE
        BINARY_PATH_NAME   : C:\Program Files (x86)\Common Files\Acronis\CDP\afcdpsrv.exe
        LOAD_ORDER_GROUP   :
        TAG                : 0
```

Reconnaissance and Footprinting

WHOIS Command:

- **Purpose:** WHOIS is used to gather information about the domain registration details of Acronis.com. This includes the registrant's name, contact information, domain creation and expiration dates, and the name servers used by the domain.
- **Findings:** Information about the domain owner, administrative and technical contacts, and the hosting provider can help in understanding the organization's external footprint and potential points of contact.

NMAP (Network Mapper):

- NMAP is used for network discovery and security auditing. It helps identify live hosts on the network, open ports, running services, and their versions, as well as possible vulnerabilities.

Recon-ng

- Recon-ng is a full-featured reconnaissance framework provides a powerful environment to gather information about a target using various modules

- **SSL/TLS Configuration**: The Qualys SSL Server Test rated Acronis.com highly, indicating strong encryption practices.
- **Security Headers**: The Security Headers Scanner revealed missing headers like Content Security Policy (CSP) and X-Content-Type-Options, which could mitigate certain types of attacks.

References

DNS Dumpster: https://dnsdumpster.com/

Netcraft Site Report: https://sitereport.netcraft.com/

ExploitDB: https://www.exploit-db.com/

CVE Details: https://cve.mitre.org/

https://security-advisory.acronis.com/advisories/SEC-7035

https://www.cve.org/CVERecord?id=CVE-2024-34013

Qualys SSL Labs: https://www.ssllabs.com/ssltest/

Security Headers: https://securityheaders.com/