SSLBoard

TLS POSTURE REPORT

SCANNED DOMAIN

airbus.com



Critical

95% of scans of similar size score higher

2026-11-05 05:37 UTC · 1,393 hostnames · 1,318 endpoints · 546 IP:port

3	10	7	
FIX NOW	FIX SOON	WORTH REVIEWING	INTERACTIVE REPORT →

Remediation plan

20 actions, in priority order. Use the numbered items to assign work, follow the remediation, and retest the affected services. Evidence and complete inventories are linked from each action.

FIX NOW · 3 ACTIONS

01 Deprecated TLS versions in use . . . 3
02 Expired certificate served . . . 3
03 Certificate expiring within 7 days . . . 3

FIX SOON · 10 ACTIONS

04 OCSP stapling needs attention . . . 4
05 Certificate expiring within 30 days . . . 4
06 DNSSEC is not configured for scoped zones . . . 4
07 Forward secrecy gaps detected . . . 5
08 Cipher suites without forward secrecy accepted . . . 5
09 Weak cipher suites detected . . . 5
10 Security header hardening gaps . . . 6
11 TLS or certificate errors . . . 6
12 Weak cipher suites on mail servers . . . 6
13 Forward secrecy gaps on mail servers . . . 7

WORTH REVIEWING · 7 ACTIONS

14 Not fully PQC ready . . . 7
15 HTTP redirects not enforced . . . 7
16 HSTS not configured . . . 8

17 RSA-only hosts . . . 8
18 Unreachable endpoints . . . 8
19 TLS 1.2 forward secrecy not confirmed on mail servers . . . 9
20 Mail servers not PQC ready . . . 9

Priority describes the original findings. Completion must be confirmed by retesting.

Technical appendix →

Fix now

3 ACTIONS

01 Deprecated TLS versions in use

168 HOSTS 540 ENDPOINTS

SSLv3, TLS 1.0 and TLS 1.1 are supported on 540 endpoints. These protocols are deprecated and expose you to known vulnerabilities.

WHAT TO CHANGE

Disable TLS 1.0, TLS 1.1 and any SSL version in the server or load balancer configuration. Keep TLS 1.2 and TLS 1.3, then confirm the older clients you still support can connect.

HOW TO VERIFY

Retest the affected services. TLS 1.0 and TLS 1.1 should be rejected while supported TLS 1.2 and TLS 1.3 connections still succeed.

Evidence on page 12 → Configuration guide →

↓ deprecated-tls.csv

02 Expired certificate served

5 ENDPOINTS

5 certificates still being served have already expired, affecting 5 endpoints. Replace immediately.

WHAT TO CHANGE

Renew and deploy a valid certificate on every endpoint that still serves the expired one. Visitors already get a browser warning on these hosts.

HOW TO VERIFY

Rescan the affected services and confirm this finding is resolved in the new report.

Evidence on page 11 → Configuration guide →

↓ certificates.csv

03 Certificate expiring within 7 days

SCOPE IN EVIDENCE

2 certificates expiring within 7 days. Renew soon to avoid outages.

WHAT TO CHANGE

Renew these certificates now and check that automated renewal actually runs for them.

HOW TO VERIFY

Rescan the affected services and confirm this finding is resolved in the new report.

Evidence on page 11 → Configuration guide →

↓ certificates.csv

Fix soon

10 ACTIONS

04 OCSP stapling needs attention

232 HOSTS 365 ENDPOINTS

365 endpoints returned partial, missing, or unknown OCSP stapling status.

EXAMPLE HOSTS [redacted].airbus.com / [redacted].airbus.com

WHAT TO CHANGE

Enable OCSP stapling on these endpoints and make sure the server can reach the OCSP responder of the CA, so clients receive a valid stapled response.

HOW TO VERIFY

Rescan the affected services and confirm this finding is resolved in the new report.

Evidence on page 12 → Configuration guide →

↓ ocsp-stapling.csv

05 Certificate expiring within 30 days

SCOPE IN EVIDENCE

14 certificates expiring within 30 days. Plan renewal.

WHAT TO CHANGE

Schedule the renewal of the certificates listed below, or confirm that automated renewal covers them, before they reach their last week. Certificates in their last week are in the item above.

HOW TO VERIFY

Rescan the affected services and confirm this finding is resolved in the new report.

Evidence on page 11 → Configuration guide →

↓ certificates.csv

06 DNSSEC is not configured for scoped zones

697 HOSTS

697 hostnames across 58 zones are not protected by DNSSEC.

EXAMPLE ZONES [redacted].cloud / [redacted].cloud

WHAT TO CHANGE

Turn on DNSSEC signing for these zones at your DNS provider and publish the DS record at your registrar.

HOW TO VERIFY

Rescan the affected services and confirm this finding is resolved in the new report.

Evidence on page 35 → Configuration guide →

↓ dnssec-issues.csv

07 Forward secrecy gaps detected

15 HOSTS 397 ENDPOINTS

15 hosts cannot establish forward-secure connections, allowing passive observers to decrypt captured traffic if the private key is later compromised.

EXAMPLE HOSTS [redacted].airbus.com / [redacted].airbus.com

WHAT TO CHANGE
Prefer ECDHE key exchange on these hosts and remove the cipher suites that use static RSA key exchange.

HOW TO VERIFY
Rescan the affected services and confirm this finding is resolved in the new report.

Evidence on page 25 → Configuration guide →

↓ forward-secrecy-gaps.csv

08 Cipher suites without forward secrecy accepted

167 HOSTS 382 ENDPOINTS

167 hosts accept RSA key exchange cipher suites, so clients that offer them connect without forward secrecy, allowing passive observers to decrypt captured traffic if the private key is later compromised.

EXAMPLE HOSTS [redacted].airbus.com / [redacted].airbus.com

WHAT TO CHANGE
Remove the cipher suites that use static RSA key exchange (TLS_RSA_WITH_*) and keep ECDHE suites for TLS 1.2 clients.

HOW TO VERIFY
Rescan the affected services and confirm this finding is resolved in the new report.

Evidence on page 25 → Configuration guide →

↓ forward-secrecy-gaps.csv

09 Weak cipher suites detected

298 HOSTS 552 ENDPOINTS

552 endpoints across 298 hosts negotiate weak or deprecated cipher suites, reducing transport security.

EXAMPLE HOSTS [redacted].airbus.com

WHAT TO CHANGE
Remove the cipher suites listed below from the server configuration and keep AEAD suites such as AES-GCM and ChaCha20-Poly1305.

HOW TO VERIFY
Rescan the affected services and confirm this finding is resolved in the new report.

Evidence on page 14 → Configuration guide →

↓ weak-ciphers.csv

10 Security header hardening gaps

600 HOSTS 1808 ENDPOINTS

1648 findings across 600 hosts include missing or weak CSP, frame protection, nosniff, or cookie security controls.

EXAMPLE HOSTS airbus.com / [redacted].airbus.com

WHAT TO CHANGE
Add the missing Content-Security-Policy, frame protection and X-Content-Type-Options headers, and set Secure, HttpOnly and SameSite on cookies, host by host as listed below.

HOW TO VERIFY
Rescan the affected services and confirm this finding is resolved in the new report.

Evidence on page 27 → Configuration guide →

↓ security-headers.csv

11 TLS or certificate errors

23 HOSTS 32 ENDPOINTS

32 endpoints across 23 hosts returned TLS handshake or certificate errors. These indicate real misconfigurations that should be investigated.

WHAT TO CHANGE
Fix the handshake or certificate error reported for each endpoint below. Hostname mismatches, incomplete chains and self-signed certificates are the usual causes.

HOW TO VERIFY
Rescan the affected services and confirm this finding is resolved in the new report.

Evidence on page 31 → Configuration guide →

↓ tls-errors.csv ↓ certificate-errors.csv

12 Weak cipher suites on mail servers

2 HOSTS 2 ENDPOINTS

2 mail endpoints across 2 MX hosts negotiate weak or deprecated cipher suites, reducing transport security.

EXAMPLE HOSTS [redacted].net / [redacted].net

WHAT TO CHANGE
Remove weak cipher suites from the TLS configuration of these mail servers.

HOW TO VERIFY
Rescan the affected services and confirm this finding is resolved in the new report.

Evidence on page 43 → Configuration guide →

↓ email-security-smtp.csv ↓ email-security-findings.csv

13 Forward secrecy gaps on mail servers

1 HOST 1 ENDPOINT

1 mail endpoint accept connections without forward secrecy, through RSA key exchange or a missing ECDHE/DHE suite, allowing passive observers to decrypt captured traffic if the private key is later compromised.

WHAT TO CHANGE
Prefer ECDHE key exchange on these mail servers and remove static RSA key exchange.

HOW TO VERIFY
Rescan the affected services and confirm this finding is resolved in the new report.

Evidence on page 43 → Configuration guide →

↓ email-security-smtp.csv ↓ email-security-findings.csv

Worth reviewing

7 ACTIONS

14 Not fully PQC ready

167 HOSTS 170 ENDPOINTS

170 endpoints are not yet post-quantum ready. Consider enabling PQC key exchange where supported.

EXAMPLE HOSTS [redacted].airbus.com / [redacted].airbus.com

WHAT TO CHANGE
Enable a hybrid post-quantum key exchange such as X25519MLKEM768 wherever your TLS stack supports it.

HOW TO VERIFY
Rescan the affected services and confirm this finding is resolved in the new report.

Evidence on page 34 → Configuration guide →

↓ pqc-not-ready.csv

15 HTTP redirects not enforced

19 HOSTS 19 ENDPOINTS

19 hosts serving HTTP on port 80 do not redirect to HTTPS.

EXAMPLE HOSTS [redacted].airbus.com / [redacted].[redacted].airbus.com

WHAT TO CHANGE
Redirect plain HTTP on port 80 to HTTPS with a permanent 301 or 308 response.

HOW TO VERIFY
Request each affected host over HTTP and confirm it redirects to the intended HTTPS URL, then rescan.

Evidence on page 27 → Configuration guide →

↓ http-hardening.csv

16 HSTS not configured

160 HOSTS 160 ENDPOINTS

160 hosts do not serve HSTS headers.

EXAMPLE HOSTS [redacted].airbus.com / [redacted].airbus.com

WHAT TO CHANGE
Send a Strict-Transport-Security header on HTTPS responses. Start with a short max-age and raise it once every subdomain works over HTTPS.

HOW TO VERIFY
Confirm the HTTPS response includes the intended Strict-Transport-Security header, then rescan.

Evidence on page 27 → Configuration guide →

↓ http-hardening.csv

17 RSA-only hosts

707 HOSTS 999 ENDPOINTS

707 hosts present only RSA certificates (no ECDSA certificates observed). Consider enabling ECDSA certificates for modern client performance and agility.

EXAMPLE HOSTS airbus.com / [redacted].airbus.com

WHAT TO CHANGE
Deploy an ECDSA certificate next to the RSA one so modern clients get smaller, faster handshakes.

HOW TO VERIFY
Rescan the affected services and confirm this finding is resolved in the new report.

Evidence on page 26 → Configuration guide →

↓ rsa-only.csv

18 Unreachable endpoints

643 HOSTS 657 ENDPOINTS

643 hosts could not be reached (DNS failures, private address resolution, timeouts, or other connectivity issues).

WHAT TO CHANGE
Check whether these hostnames are still in use and remove the DNS records that point to retired services.

HOW TO VERIFY
Confirm which hostnames are active before removing records. Rescan active services from the intended network; public reachability is not required for intentionally private services.

Evidence on page 31 → Configuration guide →

↓ dns-errors.csv ↓ private-address-errors.csv ↓ connection-errors.csv ↓ other-errors.csv

19 TLS 1.2 forward secrecy not confirmed on mail servers

1 HOST 1 ENDPOINT

1 mail endpoint support TLS 1.2 or older, but neither an ECDHE nor an RSA key exchange suite could be negotiated. The server may use suites the scanner does not offer, such as DHE; review its TLS 1.2 cipher configuration.

WHAT TO CHANGE

List the TLS 1.2 cipher suites these mail servers accept and confirm they all use ECDHE or DHE key exchange.

HOW TO VERIFY

Rescan the affected services and confirm this finding is resolved in the new report.

Evidence on page 43 → Configuration guide →

↓ email-security-smtp.csv ↓ email-security-findings.csv

20 Mail servers not PQC ready

2 HOSTS 2 ENDPOINTS

2 mail endpoints are not yet post-quantum ready. Consider enabling PQC key exchange where supported.

WHAT TO CHANGE

Enable a hybrid post-quantum key exchange on these mail servers once the TLS library of your MTA supports it.

HOW TO VERIFY

Rescan the affected services and confirm this finding is resolved in the new report.

Evidence on page 43 → Configuration guide →

↓ email-security-smtp.csv ↓ email-security-findings.csv

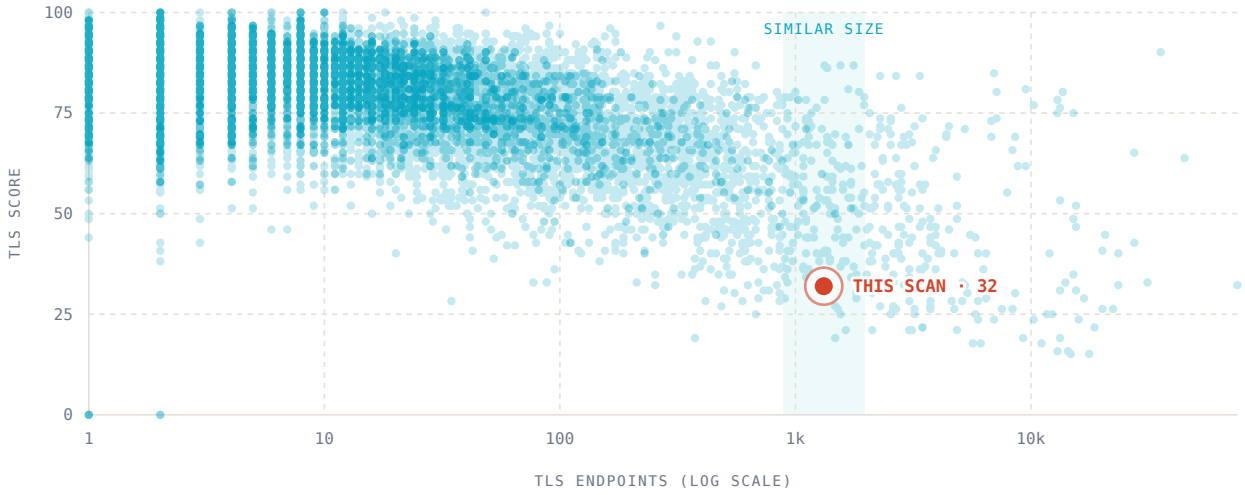
Technical appendix

Supporting observations and evidence from the original scan. Use the remediation plan for the order of work.

How this scan compares

95% of scans of similar size score higher

Each dot is a completed SSLBoard scan, placed by endpoint count and TLS score. The red marker is this report. The shaded band marks scans of similar size, which the ranking is drawn from.



What drives the score

Each category is scored out of 100 and counts toward the total by its weight. Points lost is the shortfall from 100 multiplied by the weight, so a weak category with a small weight can cost less than a stronger one with a large weight. Categories are ordered by points lost.

CATEGORY	POINTS LOST	POINTS	CATEGORY SCORE	WEIGHT
Certificate Health		−17.1	43/100	30%
Ciphers		−14.0	7/100	15%
Protocols		−13.8	8/100	15%
Confidentiality and Agility		−10.0	50/100	20%
Web Hardening		−9.4	6/100	10%
Future Readiness		−2.2	57/100	5%
Reliability		−2.0	60/100	5%

Strengths

✓

TLS 1.3 support
1019 of 1112 endpoints (92%) support TLS 1.3.

✓

Strong certificate keys
All 291 active certificates use strong keys (RSA 2048+, P-256+, or Ed25519/Ed448).

✓

Certificate issuer diversity
6 trusted CAs in rotation for non-expired certificates, which supports redundancy and renewal flexibility.

1 Certificates

Certificates are a common source of operational risk when they are hard to track, inconsistently issued, or close to expiry. This section helps you review the certificates observed on reachable endpoints so you can spot renewal risk, issuer sprawl, and inconsistencies across the estate.

↓ Download certificate inventory (CSV)

↓ Download CAA policies (CSV)

1.1 Certificates Nearing Expiration

Certificates close to expiry increase the risk of avoidable outages and rushed renewals. This section highlights which observed certificates need attention soon so renewal work can be prioritized before service is affected.

5	2	4	8	288
Already expired	Within 7 days	8 to 15 days	16 to 30 days	31 days or more

19 certificates of the 307 in use are expired or expire within 30 days, and 5 certificates still are served after expiry.

1.2 Issuer Distribution



DigiCert Inc	157	52%
Google Trust Services	82	27%
Let's Encrypt	29	10%
GlobalSign nv-sa	20	7%
Amazon	13	4%
Internal corporate CA	1	0%

1.3 CAA Policies

CAA records let a domain specify which certificate authorities are allowed to issue certificates for it. Use this section to confirm whether issuance is restricted, identify gaps where no policy is published, and spot inconsistent rules across subdomains.

NAME	ALLOWED ISSUERS	WILDCARD ISSUERS
[redacted].airbus.com	letsencrypt.org	*Same as allowed*

2 TLS Protocols & Versions

This section shows which TLS versions are supported across your scanned endpoints. In general, support for modern versions such as TLS 1.2 and TLS 1.3 is expected, while older versions like SSLv3, TLS 1.0, and TLS 1.1 should usually be disabled because they are outdated and may expose you to security, compliance, or compatibility issues.

↓ Download per-IP TLS details (CSV)

SSLV3	TLS 1.0	TLS 1.1	TLS 1.2	TLS 1.3
2 endpoints, deprecated	268 endpoints, deprecated	270 endpoints, deprecated	1043 endpoints	1019 endpoints

2.2 Deprecated TLS Versions

SSLv3 2 endpoints across 2 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

↓ Download sslv3 (CSV)

TLS1.0 268 endpoints across 82 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443 [redacted] [redacted] *and 5 more in CSV*
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 82 hostnames. Download the CSV for the full list.

↓ Download tls1.0 (CSV)

TLS1.1 270 endpoints across 84 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443 [redacted] [redacted] *and 5 more in CSV*
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 84 hostnames. Download the CSV for the full list.

↓ Download tls1.1 (CSV)

2.3 Missing TLS 1.3

TLS 1.3 is the current baseline for modern HTTPS. This subsection highlights endpoints that still stop at older TLS versions, which can increase latency, limit access to newer security improvements, and leave parts of the estate behind current hardening standards.

Endpoints missing TLS 1.3 93 endpoints across 82 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 82 hostnames. Download the CSV for the full list.
↓ Download endpoints missing tls 1.3 (CSV)

2.4 OCSP Stapling

OCSP stapling lets the server attach certificate status during the TLS handshake. These endpoint-level results show where stapling is valid, missing, not available from the CA, partial, stale, invalid, or reporting a revocation problem.

423 Full	0 Partial	365 Not stapled	323 Not Available
0 Expired	0 Unknown	0 Bogus	0 Revoked

OCSP stapling issues 365 endpoints across 232 hostnames

HOSTNAME	IP : PORT	ISSUE
[redacted].airbus.com	[redacted]:443	Not stapled (Info) The server doesn't attach OCSP status to its handshake. SSLBoard checks revocation separately.
[redacted].airbus.com	[redacted]:443	Not stapled (Info) The server doesn't attach OCSP status to its handshake. SSLBoard checks revocation separately.
[redacted].airbus.com	[redacted]:443	Not stapled (Info) The server doesn't attach OCSP status to its handshake. SSLBoard checks revocation separately.
[redacted].airbus.com	[redacted]:443	Not stapled (Info) The server doesn't attach OCSP status to its handshake. SSLBoard checks revocation separately.

Showing 4 of 232 hostnames. Download the CSV for the full list.
↓ Download ocsp stapling issues (CSV)

3 Weak Cipher Suites

This section identifies weak or outdated cipher suites detected across your scanned endpoints. These ciphers can reduce transport security by relying on obsolete encryption, weak key exchange, or legacy integrity mechanisms, which may increase exposure to known attacks and create compliance risk.

↓ Download weak ciphers (CSV)

TLS_RSA_EXPORT_WITH_RC4_40_MD5 1 endpoint across 1 hostname

HOSTNAME	IP : PORT
██████.airbus.com	███.█.██.███:443

↓ Download tls_rsa_export_with_rc4_40_md5 (CSV)

TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA 1 endpoint across 1 hostname

HOSTNAME	IP : PORT
██████.airbus.com	███.█.██.███:443

↓ Download tls_dhe_rsa_export_with_des40_cbc_sha (CSV)

TLS_RSA_EXPORT_WITH_DES40_CBC_SHA 1 endpoint across 1 hostname

HOSTNAME	IP : PORT
██████.airbus.com	███.█.██.███:443

↓ Download tls_rsa_export_with_des40_cbc_sha (CSV)

TLS_RSA_WITH_RC4_128_MD5 4 endpoints across 4 hostnames

HOSTNAME	IP : PORT
██████████.airbus.com	███.███.███.██:443
████████████.airbus.com	███.███.███.██:443
██████.airbus.com	███.█.██.███:443
██████████.███.airbus.com	██.███.███.███:443

↓ Download tls_rsa_with_rc4_128_md5 (CSV)

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA 1 endpoint across 1 hostname

HOSTNAME	IP : PORT
██████.airbus.com	███.█.██.███:443

↓ Download tls_dhe_rsa_with_3des_ede_cbc_sha (CSV)

TLS_DHE_RSA_WITH_DES_CBC_SHA 1 endpoint across 1 hostname

HOSTNAME	IP : PORT
██████.airbus.com	███.█.██.███:443

↓ Download tls_dhe_rsa_with_des_cbc_sha (CSV)

TLS_RSA_WITH_3DES_EDE_CBC_SHA 260 endpoints across 82 hostnames

HOSTNAME	IP : PORT
███████.airbus.com	███.███.██.██:443 ████:████:████:██::██:███ ████:████:████:██::██:███ *and 5 more in CSV*
████████████.airbus.com	███.█.██.███:443

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 82 hostnames. Download the CSV for the full list.
↓ Download tls_rsa_with_3des_ede_cbc_sha (CSV)

TLS_RSA_WITH_DES_CBC_SHA 1 endpoint across 1 hostname

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443

↓ Download tls_rsa_with_des_cbc_sha (CSV)

TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA 1 endpoint across 1 hostname

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443

↓ Download tls_ecdhe_rsa_with_3des_ede_cbc_sha (CSV)

TLS_RSA_WITH_RC4_128_SHA 4 endpoints across 4 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

↓ Download tls_rsa_with_rc4_128_sha (CSV)

TLS_DHE_RSA_WITH_AES_128_CBC_SHA 26 endpoints across 26 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 26 hostnames. Download the CSV for the full list.
↓ Download tls_dhe_rsa_with_aes_128_cbc_sha (CSV)

TLS_DHE_RSA_WITH_AES_256_CBC_SHA 25 endpoints across 25 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 25 hostnames. Download the CSV for the full list.
↓ Download tls_dhe_rsa_with_aes_256_cbc_sha (CSV)

TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA 20 endpoints across 20 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443

Showing 4 of 20 hostnames. Download the CSV for the full list.
↓ Download tls_dhe_rsa_with_camellia_128_cbc_sha (CSV)

TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA 20 endpoints across 20 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 20 hostnames. Download the CSV for the full list.
↓ Download tls_dhe_rsa_with_camellia_256_cbc_sha (CSV)

TLS_RSA_WITH_AES_128_CBC_SHA 343 endpoints across 149 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 149 hostnames. Download the CSV for the full list.
↓ Download tls_rsa_with_aes_128_cbc_sha (CSV)

TLS_RSA_WITH_AES_256_CBC_SHA 345 endpoints across 151 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 151 hostnames. Download the CSV for the full list.
↓ Download tls_rsa_with_aes_256_cbc_sha (CSV)

TLS_RSA_WITH_CAMELLIA_128_CBC_SHA 33 endpoints across 33 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 33 hostnames. Download the CSV for the full list.
↓ Download tls_rsa_with_camellia_128_cbc_sha (CSV)

TLS_RSA_WITH_CAMELLIA_256_CBC_SHA 33 endpoints across 33 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443

Showing 4 of 33 hostnames. Download the CSV for the full list.
↓ Download tls_rsa_with_camellia_256_cbc_sha (CSV)

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 53 endpoints across 53 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 53 hostnames. Download the CSV for the full list.
↓ Download tls_dhe_rsa_with_aes_128_cbc_sha256 (CSV)

TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 53 endpoints across 53 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 53 hostnames. Download the CSV for the full list.
↓ Download tls_dhe_rsa_with_aes_256_cbc_sha256 (CSV)

TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 19 endpoints across 19 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 19 hostnames. Download the CSV for the full list.
↓ Download tls_dhe_rsa_with_camellia_128_cbc_sha256 (CSV)

TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256 19 endpoints across 19 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 19 hostnames. Download the CSV for the full list.
↓ Download tls_dhe_rsa_with_camellia_256_cbc_sha256 (CSV)

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA 10 endpoints across 10 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443

Showing 4 of 10 hostnames. Download the CSV for the full list.
↓ Download tls_ecdhe_ecdsa_with_aes_128_cbc_sha (CSV)

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA 10 endpoints across 10 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 10 hostnames. Download the CSV for the full list.
↓ Download tls_ecdhe_ecdsa_with_aes_256_cbc_sha (CSV)

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA 409 endpoints across 213 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 213 hostnames. Download the CSV for the full list.
↓ Download tls_ecdhe_rsa_with_aes_128_cbc_sha (CSV)

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA 407 endpoints across 212 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 212 hostnames. Download the CSV for the full list.
↓ Download tls_ecdhe_rsa_with_aes_256_cbc_sha (CSV)

TLS_RSA_WITH_AES_128_CBC_SHA256 141 endpoints across 111 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 111 hostnames. Download the CSV for the full list.
↓ Download tls_rsa_with_aes_128_cbc_sha256 (CSV)

TLS_RSA_WITH_AES_256_CBC_SHA256 121 endpoints across 108 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443

Showing 4 of 108 hostnames. Download the CSV for the full list.
↓ Download tls_rsa_with_aes_256_cbc_sha256 (CSV)

TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256 2 endpoints across 2 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

↓ Download tls_rsa_with_camellia_128_cbc_sha256 (CSV)

TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256 2 endpoints across 2 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

↓ Download tls_rsa_with_camellia_256_cbc_sha256 (CSV)

TLS_DHE_RSA_WITH_AES_128_CCM 20 endpoints across 20 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 20 hostnames. Download the CSV for the full list.
↓ Download tls_dhe_rsa_with_aes_128_ccm (CSV)

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 65 endpoints across 65 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 65 hostnames. Download the CSV for the full list.
↓ Download tls_dhe_rsa_with_aes_128_gcm_sha256 (CSV)

TLS_DHE_RSA_WITH_AES_256_CCM 20 endpoints across 20 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 20 hostnames. Download the CSV for the full list.
↓ Download tls_dhe_rsa_with_aes_256_ccm (CSV)

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 66 endpoints across 66 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 66 hostnames. Download the CSV for the full list.
↓ Download tls_dhe_rsa_with_aes_256_gcm_sha384 (CSV)

TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256 19 endpoints across 19 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 19 hostnames. Download the CSV for the full list.
↓ Download tls_dhe_rsa_with_aria_128_gcm_sha256 (CSV)

TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384 19 endpoints across 19 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 19 hostnames. Download the CSV for the full list.
↓ Download tls_dhe_rsa_with_aria_256_gcm_sha384 (CSV)

TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 24 endpoints across 24 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 24 hostnames. Download the CSV for the full list.
↓ Download tls_dhe_rsa_with_chacha20_poly1305_sha256 (CSV)

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 35 endpoints across 13 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 13 hostnames. Download the CSV for the full list.
↓ Download tls_ecdhe_ecdsa_with_aes_128_cbc_sha256 (CSV)

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 36 endpoints across 14 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443

HOSTNAME	IP : PORT
███.██████.█████.airbus.com	██.██.██.██:443
██.████.██████.█████.airbus.com	██.██.██.██:443
████████.██████.█████.airbus.com	██.██.██.██:443

Showing 4 of 14 hostnames. Download the CSV for the full list.
↓ Download tls_ecdhe_ecdsa_with_aes_256_cbc_sha384 (CSV)

TLS_ECDHE_ECDSA_WITH_CAMELLIA_128_CBC_SHA256 10 endpoints across 10 hostnames

HOSTNAME	IP : PORT
███.██████.█████.airbus.com	██.██.██.██:443
███.██████.█████.airbus.com	██.██.██.██:443
██.████.██████.█████.airbus.com	██.██.██.██:443
████████.██████.█████.airbus.com	██.██.██.██:443

Showing 4 of 10 hostnames. Download the CSV for the full list.
↓ Download tls_ecdhe_ecdsa_with_camellia_128_cbc_sha256 (CSV)

TLS_ECDHE_ECDSA_WITH_CAMELLIA_256_CBC_SHA384 10 endpoints across 10 hostnames

HOSTNAME	IP : PORT
███.██████.█████.airbus.com	██.██.██.██:443
███.██████.█████.airbus.com	██.██.██.██:443
██.████.██████.█████.airbus.com	██.██.██.██:443
████████.██████.█████.airbus.com	██.██.██.██:443

Showing 4 of 10 hostnames. Download the CSV for the full list.
↓ Download tls_ecdhe_ecdsa_with_camellia_256_cbc_sha384 (CSV)

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 207 endpoints across 162 hostnames

HOSTNAME	IP : PORT
████████.airbus.com	██.██.██.██:443
████████.airbus.com	██.██.██.██:443
██████████.airbus.com	██.██.██.██:443
██████████.airbus.com	██.██.██.██:443

Showing 4 of 162 hostnames. Download the CSV for the full list.
↓ Download tls_ecdhe_rsa_with_aes_128_cbc_sha256 (CSV)

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 197 endpoints across 153 hostnames

HOSTNAME	IP : PORT
████████.airbus.com	██.██.██.██:443
████████.airbus.com	██.██.██.██:443
██████████.airbus.com	██.██.██.██:443
██████████.airbus.com	██.██.██.██:443

Showing 4 of 153 hostnames. Download the CSV for the full list.
↓ Download tls_ecdhe_rsa_with_aes_256_cbc_sha384 (CSV)

TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 28 endpoints across 28 hostnames

HOSTNAME	IP : PORT
████████.airbus.com	██.██.██.██:443

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 28 hostnames. Download the CSV for the full list.
↓ Download tls_ecdhe_rsa_with_camellia_128_cbc_sha256 (CSV)

TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 28 endpoints across 28 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 28 hostnames. Download the CSV for the full list.
↓ Download tls_ecdhe_rsa_with_camellia_256_cbc_sha384 (CSV)

TLS_RSA_WITH_AES_128_CCM 3 endpoints across 3 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

↓ Download tls_rsa_with_aes_128_ccm (CSV)

TLS_RSA_WITH_AES_128_CCM_8 1 endpoint across 1 hostname

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443

↓ Download tls_rsa_with_aes_128_ccm_8 (CSV)

TLS_RSA_WITH_AES_128_GCM_SHA256 386 endpoints across 170 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 170 hostnames. Download the CSV for the full list.
↓ Download tls_rsa_with_aes_128_gcm_sha256 (CSV)

TLS_RSA_WITH_AES_256_CCM 3 endpoints across 3 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

↓ Download tls_rsa_with_aes_256_ccm (CSV)

TLS_RSA_WITH_AES_256_CCM_8 1 endpoint across 1 hostname

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443

↓ Download tls_rsa_with_aes_256_ccm_8 (CSV)

TLS_RSA_WITH_AES_256_GCM_SHA384 382 endpoints across 167 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 167 hostnames. Download the CSV for the full list.

↓ Download tls_rsa_with_aes_256_gcm_sha384 (CSV)

TLS_RSA_WITH_ARIA_128_GCM_SHA256 2 endpoints across 2 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

↓ Download tls_rsa_with_aria_128_gcm_sha256 (CSV)

TLS_RSA_WITH_ARIA_256_GCM_SHA384 2 endpoints across 2 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

↓ Download tls_rsa_with_aria_256_gcm_sha384 (CSV)

3.1 Understanding the Issues

- **3DES (Triple DES)**: CVSS 5.9 (Medium): CVE-2016-2183 covers the Sweet32 birthday attack against 64-bit block ciphers after roughly 32GB of traffic. 3DES provides only 112-bit effective security and remains vulnerable to meet-in-the-middle attacks. Its 64-bit block size makes long-lived TLS sessions especially risky. NIST SP 800-131A deprecated 3DES in 2018 and banned new uses by 2023. Disable it immediately and replace it with AES-GCM or ChaCha20-Poly1305.
- **RC4**: CVSS 4.3-5.0 (Medium): notable examples include CVE-2013-2566 for Fluhrer-McGrew keystream biases and CVE-2015-2808 for the Bar Mitzvah attack. RC4 is fully unsafe. Its biased keystream makes plaintext recovery practical, with some attacks becoming feasible after around 1GB of traffic. RFC 7465 banned RC4 in TLS in 2015. It should not appear in any modern TLS configuration. Replace it with AES-GCM or ChaCha20-Poly1305.
- **EXPORT Ciphers**: EXPORT ciphers provide only trivially weak 40/56-bit protection, crackable in hours via modern hardware. Legacy U.S. export restrictions created 512-bit RSA/40-bit keys (e.g., EXP1024-* suites). Banned since 2015 (RFC 7465); enabling them fails PCI-DSS and most compliance.
- **MD5**: CVSS 5.9 (Medium): CVE-2012-0397 covered the Flame malware certificate forgery case built on MD5 collision attacks. MD5 has been practically broken for a long time, with real collision attacks known since 2004. It is unsuitable for signatures, certificate validation, or security-sensitive hashing. Beyond collisions, MD5 also suffers from length-extension weaknesses in constructions that were never designed to resist them. MD5 should be removed from TLS and replaced with SHA-256 or stronger algorithms.
- **DES**: DES uses an obsolete key size, and DES40 is deliberately export-grade. Both are far below modern TLS security requirements. Disable DES suites and keep only AEAD ciphers such as AES-GCM or ChaCha20-Poly1305.
- **CBC Mode**: CVSS 5.9-7.5 (Medium/High): key examples include CVE-2011-3389 for BEAST and CVE-2013-0169 for Lucky Thirteen. CBC mode in TLS 1.0-1.2 has a long history of timing leaks, padding oracles, and related side-channel attacks. Mitigations exist, but they have never made CBC a desirable modern choice. AEAD cipher suites such as AES-GCM and ChaCha20-Poly1305 avoid these structural weaknesses and should be preferred.

- **Static RSA key exchange**: TLS_RSA_WITH suites use static RSA key exchange and do not provide forward secrecy. If the server private key is compromised later, recorded TLS sessions can be at risk. Prefer TLS 1.3 or TLS 1.2 ECDHE suites.
- **Finite-field DHE**: Finite-field Diffie-Hellman Ephemeral suites are legacy TLS 1.2 choices. They are slower and easier to misconfigure than ECDHE, especially when DH parameters are weak or reused. DHE can expose servers to Logjam-style risk when parameters are too small. Even with AES-GCM and SHA-2, DHE is no longer the preferred modern baseline. Prefer TLS 1.3 and TLS 1.2 ECDHE suites with AES-GCM or ChaCha20-Poly1305. Disable DHE unless you have a documented compatibility need.
- **SHA / SHA1**: CVSS 7.5 (High): practical collision work such as SHAttered made SHA-1 unfit for modern trust decisions, and RFC 9155 deprecated it in 2022. In TLS cipher names, SHA often means SHA-1 unless a stronger variant such as SHA256 or SHA384 is named explicitly. SHA-1 is too weak for signatures and certificate-related trust. It should be disabled in modern TLS deployments in favor of SHA-256 or SHA-384.

4 Forward Secrecy Analysis

Forward secrecy means that a server's long-term private key alone should not be enough to decrypt previously recorded TLS sessions. In practice, this usually requires TLS 1.3 or older TLS versions configured with ECDHE or DHE cipher suites.

7 hosts
No forward secrecy

8 hosts
PFS through TLS 1.3, ECDHE/DHE ciphers missing

167 hosts
Cipher suites without forward secrecy accepted

79 hosts
No TLS 1.3, PFS with ECDHE/DHE ciphers

34 hosts
TLS 1.3 only

620 hosts
TLS 1.3 and ECDHE/DHE ciphers

⚠ 7 hosts neither support TLS 1.3 nor negotiate legacy PFS cipher suites (ECDHE/DHE). This means that if the server's private key is compromised in the future, encrypted past sessions could be decrypted.

No forward secrecy 397 endpoints across 181 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 181 hostnames. Download the CSV for the full list.
↓ Download no forward secrecy (CSV)

5 Key Analysis

5.1 Key Strength Distribution



- RSA 2048 bit RECOMMENDED — 222 76%
- RSA 4096 bit RECOMMENDED — 50 17%
- EC 256 bit (P-256) RECOMMENDED — 16 5%
- EC 384 bit (P-384) RECOMMENDED — 3 1%

5.2 RSA-Only Hosts

These hosts were observed serving only RSA certificates, with no ECDSA certificate available on the scanned endpoints. That usually means slower handshakes and larger certificates than a modern dual-stack RSA plus ECDSA setup, and it reduces cryptographic agility for future tuning.

RSA-only hosts 999 endpoints across 707 hostnames

HOSTNAME	IP : PORT
airbus.com	[redacted]:443 [redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].[redacted].airbus.com	[redacted]:443
[redacted].[redacted].airbus.com	[redacted]:443

Showing 4 of 707 hostnames. Download the CSV for the full list.

↓ Download rsa-only hosts (CSV)

6 HTTP Redirects & Security Headers

These hostname-level results focus on HTTP-to-HTTPS redirects and browser-facing HTTPS security headers observed in HTTPS responses.

557/576	450/610	137/482	228/482
HTTPS redirect coverage	HSTS coverage	CSP coverage	Frame protection

176/482	20/407
Nosniff coverage	Cookie flags

Unknown results do not count as failures. Bot protection, rate limiting, or connection errors may prevent verification. Headers of a page on another site, such as a sign-in page that this host redirects to, are also left unknown.

Unknown results 1042 endpoints across 1042 hostnames

HOSTNAME	IP : PORT	RESULT
[redacted].airbus.com	[redacted].airbus.com:443	HSTS, Security headers: Unknown The automated check could not verify this result. Bot protection, rate limiting, or a connection error may have prevented verification.
[redacted].[redacted].airbus.com	[redacted].[redacted].airbus.com:443	HSTS, Security headers: Unknown The automated check could not verify this result. Bot protection, rate limiting, or a connection error may have prevented verification.
[redacted].[redacted].airbus.com	[redacted].[redacted].airbus.com:443	HSTS, Security headers: Unknown The automated check could not verify this result. Bot protection, rate limiting, or a connection error may have prevented verification.
[redacted].[redacted].airbus.com	[redacted].[redacted].airbus.com:443	HSTS, Security headers: Unknown The automated check could not verify this result. Bot protection, rate limiting, or a connection error may have prevented verification.

Showing 4 of 1042 hostnames. Download the CSV for the full list.
↓ Download unknown results (CSV)

6.1 HTTP Redirect

Hosts that still answer over HTTP should normally redirect visitors straight to HTTPS. Without that redirect, users and automated clients can remain on an unencrypted endpoint, increasing the chance of downgrade, interception, or inconsistent application behavior.

Missing HTTP redirects 19 endpoints across 19 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted].airbus.com:443
[redacted].[redacted].airbus.com	[redacted].[redacted].airbus.com:443
[redacted].airbus.com	[redacted].airbus.com:443
[redacted].[redacted].[redacted].airbus.com	[redacted].[redacted].[redacted].airbus.com:443

Showing 4 of 19 hostnames. Download the CSV for the full list.
↓ Download missing http redirects (CSV)

6.2 HSTS

HSTS tells browsers to use HTTPS automatically for future requests and to avoid falling back to HTTP. This helps close downgrade paths after the first secure visit and reduces the risk of users being pushed onto plaintext connections.

Missing HSTS 160 endpoints across 160 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted].airbus.com:443
[redacted].airbus.com	[redacted].airbus.com:443
[redacted].airbus.com	[redacted].airbus.com:443
[redacted].airbus.com	[redacted].airbus.com:443

Showing 4 of 160 hostnames. Download the CSV for the full list.
↓ Download missing hsts (CSV)

6.3 Content Security Policy

Content Security Policy (CSP) constrains which script, style, and frame sources the browser is allowed to load. Missing or weak policies make cross-site scripting and content injection attacks easier to exploit.

CSP findings 456 endpoints across 403 hostnames

HOSTNAME	IP : PORT	ISSUE
airbus.com	airbus.com:443	Content-Security-Policy: Content Security Policy missing (Warning) No enforced CSP was observed in HTTPS responses. The headers were read from [redacted].airbus.com, where the redirects from this host end.
[redacted].airbus.com	[redacted].airbus.com:443	Content-Security-Policy: CSP is report-only (Warning) A report-only CSP does not enforce browser-side restrictions.
[redacted].airbus.com	[redacted].airbus.com:443	Content-Security-Policy: Content Security Policy missing (Warning) No enforced CSP was observed in HTTPS responses.
[redacted].airbus.com	[redacted].airbus.com:443	Content-Security-Policy: Content Security Policy missing (Warning) No enforced CSP was observed in HTTPS responses.

Showing 4 of 403 hostnames. Download the CSV for the full list.
↓ Download csp findings (CSV)

6.4 Frame Protection

Frame protection reduces clickjacking risk by preventing untrusted pages from embedding this site in iframes. These findings cover missing protection or invalid X-Frame-Options values.

Frame protection findings 254 endpoints across 254 hostnames

HOSTNAME	IP : PORT	ISSUE
airbus.com	airbus.com:443	Frame protection: Frame protection missing (Warning) Neither a valid X-Frame-Options header nor enforced CSP frame-ancestors directive was observed. The headers were read from [redacted].airbus.com, where the redirects from this host end.

HOSTNAME	IP : PORT	ISSUE
[redacted].airbus.com	[redacted].airbus.com:443	Frame protection: Frame protection missing (Warning) Neither a valid X-Frame-Options header nor enforced CSP frame-ancestors directive was observed.
[redacted].airbus.com	[redacted].airbus.com:443	Frame protection: Frame protection missing (Warning) Neither a valid X-Frame-Options header nor enforced CSP frame-ancestors directive was observed.
[redacted].airbus.com	[redacted].airbus.com:443	Frame protection: Frame protection missing (Warning) Neither a valid X-Frame-Options header nor enforced CSP frame-ancestors directive was observed.

Showing 4 of 254 hostnames. Download the CSV for the full list.
↓ Download frame protection findings (CSV)

6.5 X-Content-Type-Options (Nosniff)

X-Content-Type-Options with the nosniff value prevents browsers from MIME-sniffing responses into executable content types. Missing or invalid values increase the risk of content-type confusion attacks.

Nosniff findings 306 endpoints across 306 hostnames

HOSTNAME	IP : PORT	ISSUE
airbus.com	airbus.com:443	X-Content-Type-Options: X-Content-Type-Options missing (Warning) The response does not send the nosniff header. The headers were read from [redacted].airbus.com, where the redirects from this host end.
[redacted].airbus.com	[redacted].airbus.com:443	X-Content-Type-Options: X-Content-Type-Options missing (Warning) The response does not send the nosniff header.
[redacted].airbus.com	[redacted].airbus.com:443	X-Content-Type-Options: X-Content-Type-Options missing (Warning) The response does not send the nosniff header.
[redacted].airbus.com	[redacted].airbus.com:443	X-Content-Type-Options: X-Content-Type-Options missing (Warning) The response does not send the nosniff header.

Showing 4 of 306 hostnames. Download the CSV for the full list.
↓ Download nosniff findings (CSV)

6.6 Cookie Security Flags

Cookie security flags (Secure, HttpOnly, SameSite, and prefix rules) reduce session theft and cross-site abuse. This table highlights cookies that were observed without recommended protections.

Cookie security findings 632 endpoints across 387 hostnames

HOSTNAME	IP : PORT	ISSUE
airbus.com	airbus.com:443	Cookies: Cookie missing HttpOnly (Warning) At least one Set-Cookie header omitted the HttpOnly attribute.
[redacted].airbus.com	[redacted].airbus.com:443	Cookies: Cookie missing HttpOnly (Warning) At least one Set-Cookie header omitted the HttpOnly attribute.
[redacted].airbus.com	[redacted].airbus.com:443	Cookies: Cookie missing SameSite (Warning) At least one Set-Cookie header omitted a SameSite policy.

HOSTNAME	IP : PORT	ISSUE
[redacted].airbus.com	[redacted].airbus.com:443 [redacted].airbus.com:443	Cookies: Cookie missing HttpOnly (Warning) At least one Set-Cookie header omitted the HttpOnly attribute. Cookies: Cookie missing SameSite (Warning) At least one Set-Cookie header omitted a SameSite policy.

Showing 4 of 387 hostnames. Download the CSV for the full list.

↓ Download cookie security findings (CSV)

7 Connection & Certificate Errors

These errors and warnings prevented SSLBoard from establishing a valid TLS connection. As a result, we could not verify which certificate those endpoints are serving, or whether they are serving the correct one. In most cases, these are operational issues rather than direct security problems, but they can still lead to service disruption or unavailability.

7.1 DNS Resolution Errors

These are hostnames that appear in your SSL certificates but do not exist in your public DNS.

DNS Resolution Errors 451 endpoints across 451 hostnames

HOSTNAME	IP : PORT	ISSUE
[redacted].airbus.com	<no ip>:443	dns lookup returned no addresses
[redacted].airbus.com	<no ip>:443	dns lookup returned no addresses
[redacted].airbus.com	<no ip>:443	dns lookup returned no addresses
[redacted].airbus.com	<no ip>:443	dns lookup returned no addresses

Showing 4 of 451 hostnames. Download the CSV for the full list.
↓ Download dns resolution errors (CSV)

7.2 Private Address Resolution

These are hostnames that resolve to private or internal IP addresses and therefore are intentionally not scanned from SSLBoard's public worker.

Private Address Resolution 6 endpoints across 6 hostnames

HOSTNAME	IP : PORT	ISSUE
[redacted].airbus.com	<no ip>:443	hostname resolves to a private address
[redacted].airbus.com	<no ip>:443	hostname resolves to a private address
[redacted].airbus.com	<no ip>:443	hostname resolves to a private address
[redacted].airbus.com	<no ip>:443	hostname resolves to a private address

Showing 4 of 6 hostnames. Download the CSV for the full list.
↓ Download private address resolution (CSV)

7.3 Connection & Timeout Errors

These are hostnames that appear in your SSL certificates and in your DNS, but the server is not responding. Common reasons include internal systems that are not reachable from the public Internet, firewall rules, server downtime, or stale DNS records that still point to a host that no longer serves HTTPS on port 443.

Connection & Timeout Errors 186 endpoints across 172 hostnames

HOSTNAME	IP : PORT	ISSUE
[redacted].airbus.com	[redacted]:443	dial tcp [redacted]:443: i/o timeout
[redacted].airbus.com	[redacted]:443	dial tcp [redacted]:443: i/o timeout

HOSTNAME	IP : PORT	ISSUE
[redacted].airbus.com	[redacted]:443	dial tcp [redacted]:443: i/o timeout
[redacted].airbus.com	[redacted]:443	dial tcp [redacted]:443: i/o timeout

Showing 4 of 172 hostnames. Download the CSV for the full list.
↓ Download connection & timeout errors (CSV)

7.4 TLS Handshake Errors

These are servers for which we could not successfully complete the SSL/TLS handshake. This is usually worth investigating, as it often points to a real configuration or compatibility issue.

TLS Handshake Errors 5 endpoints across 4 hostnames

HOSTNAME	IP : PORT	ISSUE
[redacted].airbus.com	[redacted]:443	remote error: tls: handshake failure
[redacted].airbus.com	[redacted]:443	remote error: tls: handshake failure
[redacted].airbus.com	[redacted]:443	remote error: tls: handshake failure
[redacted].airbus.com	[redacted]:443 [redacted]:443	tls: first record does not look like a TLS handshake

↓ Download tls handshake errors (CSV)

7.5 Certificate Errors

These servers appear to be misconfigured. For example, they may be sending an incomplete certificate chain, or they may be presenting a certificate that is not valid for the requested hostname. These issues should be investigated.

Note: this can also become a security risk if dependent systems work around the problem by weakening TLS validation, for example by disabling certificate validation entirely.

Certificate Errors 27 endpoints across 19 hostnames

HOSTNAME	IP : PORT	ISSUE
[redacted].airbus.com	[redacted]:443	x509: certificate is valid for [redacted].airbus.com, [redacted].airbus.com, not [redacted].airbus.com
[redacted].airbus.com	[redacted]:443	x509: certificate is valid for [redacted].airbus.com, [redacted].airbus.com, not [redacted].airbus.com
[redacted].airbus.com	[redacted]:443	x509: certificate is valid for [redacted].airbus.com, [redacted].airbus.com, not [redacted].airbus.com
[redacted].airbus.com	[redacted]:443	Certificate is expired

Showing 4 of 19 hostnames. Download the CSV for the full list.
↓ Download certificate errors (CSV)

7.6 Other Errors

These are servers we could not connect to for reasons that did not fit the categories above. They should be reviewed and investigated.

Other Errors 14 endpoints across 14 hostnames

HOSTNAME	IP : PORT	ISSUE
[redacted].airbus.com	[redacted]:443	EOF
[redacted].airbus.com	[redacted]:443	remote error: tls: unrecognized name
[redacted]. airbus.com	[redacted]:443	dial tcp [redacted]:443: connect: no route to host
[redacted].airbus.com	[redacted]:443	dial tcp [redacted]:443: connect: no route to host

Showing 4 of 14 hostnames. Download the CSV for the full list.

↓ Download other errors (CSV)

8 PQC Readiness Summary

This section summarizes how prepared your scanned endpoints are for post-quantum cryptography. It highlights the proportion of endpoints already aligned with PQC readiness expectations and surfaces the remaining gaps so you can prioritize remediation before quantum-safe requirements become operational or compliance-driven.

high
Readiness

83%
of 1009 endpoints ready

170
Endpoints not PQC-ready

309
119 errored

PQC Groups

839 endpoints
X25519+MLKEM768

Non-PQC-ready endpoints 170 endpoints across 167 hostnames

HOSTNAME	IP : PORT
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443
[redacted].airbus.com	[redacted]:443

Showing 4 of 167 hostnames. Download the CSV for the full list.
↓ Download non-pqc-ready endpoints (CSV)

9 DNSSEC

DNSSEC protects your domains against DNS spoofing by cryptographically signing responses. Below are the zones we found, their signing status, and any issues that need attention.

6
Secure zones

58
Insecure zones

4
Error zones

310
Protected hostnames

697
Unprotected hostnames

DNSSEC issues 63 endpoints across 63 hostnames

HOSTNAME	IP : PORT	ISSUE
[redacted].cloud	1 hostname	DNSSEC is not configured Zone [redacted].cloud has no DNSSEC configured (no DS record in parent zone [redacted].cloud). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
[redacted].cloud	1 hostname	DNSSEC is not configured Zone [redacted].cloud has no DNSSEC configured (no DS record in parent zone [redacted].cloud). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
[redacted].cloud	9 hostnames	DNSSEC is not configured Zone [redacted].cloud has no DNSSEC configured (no DS record in parent zone [redacted].cloud). This is common but means DNS responses for 9 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
[redacted].cloud	9 hostnames	No DNSSEC configured

Showing 4 of 63 hostnames. Download the CSV for the full list.
↓ Download dnssec issues (CSV)

Per-zone status

- INSECURE [redacted].cloud: 1 hostname
  - INFO **DNSSEC is not configured**: Zone [redacted].cloud has no DNSSEC configured (no DS record in parent zone [redacted].cloud). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].cloud: 1 hostname
  - INFO **DNSSEC is not configured**: Zone [redacted].cloud has no DNSSEC configured (no DS record in parent zone [redacted].cloud). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].cloud: 9 hostnames

- INFO **DNSSEC is not configured**: Zone [redacted].cloud has no DNSSEC configured (no DS record in parent zone [redacted].cloud). This is common but means DNS responses for 9 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- ERROR [redacted].**cloud**: 9 hostnames
- ERROR [redacted].**cloud**: 9 hostnames
- INSECURE [redacted].**cloud**: 9 hostnames
  - INFO **DNSSEC is not configured**: Zone [redacted].cloud has no DNSSEC configured (no DS record in parent zone [redacted].cloud). This is common but means DNS responses for 9 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].**cloud**: 1 hostname
  - INFO **DNSSEC is not configured**: Zone [redacted].cloud has no DNSSEC configured (no DS record in parent zone [redacted].cloud). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].**cloud**: 1 hostname
  - INFO **DNSSEC is not configured**: Zone [redacted].cloud has no DNSSEC configured (no DS record in parent zone [redacted].cloud). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].**akamaiedge.net**: 10 hostnames
  - INFO **DNSSEC is not configured**: Zone [redacted].akamaiedge.net has no DNSSEC configured (no DS record in parent zone akamaiedge.net). This is common but means DNS responses for 10 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].**cloud**: 1 hostname
  - INFO **DNSSEC is not configured**: Zone [redacted].cloud has no DNSSEC configured (no DS record in parent zone [redacted].cloud). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].**cloud**: 8 hostnames
  - INFO **DNSSEC is not configured**: Zone [redacted].cloud has no DNSSEC configured (no DS record in parent zone cloud). This is common but means DNS responses for 8 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE **airbus.com**: 246 hostnames
  - INFO **DNSSEC is not configured**: Zone airbus.com has no DNSSEC configured (no DS record in parent zone com). This is common but means DNS responses for 246 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE **akadns.net**: 1 hostname
  - INFO **DNSSEC is not configured**: Zone akadns.net has no DNSSEC configured (no DS record in parent zone net). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].**cloud**: 1 hostname
  - INFO **DNSSEC is not configured**: Zone [redacted].cloud has no DNSSEC configured (no DS record in parent zone [redacted].cloud). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.

- INSECURE [redacted].cloud: 9 hostnames
  - INFO **DNSSEC is not configured**: Zone [redacted].cloud has no DNSSEC configured (no DS record in parent zone [redacted].cloud). This is common but means DNS responses for 9 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].akamaiedge.net: 1 hostname
  - INFO **DNSSEC is not configured**: Zone [redacted].akamaiedge.net has no DNSSEC configured (no DS record in parent zone akamaiedge.net). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].airbus.com: 1 hostname
  - INFO **DNSSEC is not configured**: Zone [redacted].airbus.com has no DNSSEC configured (no DS record in parent zone airbus.com). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].com: 9 hostnames
  - INFO **DNSSEC is not configured**: Zone [redacted].com has no DNSSEC configured (no DS record in parent zone [redacted].com). This is common but means DNS responses for 9 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].com: 2 hostnames
  - INFO **DNSSEC is not configured**: Zone [redacted].com has no DNSSEC configured (no DS record in parent zone [redacted].com). This is common but means DNS responses for 2 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE **cloudfront.net**: 1 hostname
  - INFO **DNSSEC is not configured**: Zone cloudfront.net has no DNSSEC configured (no DS record in parent zone net). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].akasripcn.net: 2 hostnames
  - INFO **DNSSEC is not configured**: Zone [redacted].akasripcn.net has no DNSSEC configured (no DS record in parent zone akasripcn.net). This is common but means DNS responses for 2 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].com: 3 hostnames
  - INFO **DNSSEC is not configured**: Zone [redacted].com has no DNSSEC configured (no DS record in parent zone [redacted].com). This is common but means DNS responses for 3 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].akamaiedge.net: 2 hostnames
  - INFO **DNSSEC is not configured**: Zone [redacted].akamaiedge.net has no DNSSEC configured (no DS record in parent zone akamaiedge.net). This is common but means DNS responses for 2 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].cloudfront.net: 1 hostname
  - INFO **DNSSEC is not configured**: Zone [redacted].cloudfront.net has no DNSSEC configured (no DS record in parent zone cloudfront.net). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.

- INSECURE [redacted].cloudfront.net: 2 hostnames
  - INFO **DNSSEC is not configured**: Zone [redacted].cloudfront.net has no DNSSEC configured (no DS record in parent zone cloudfront.net). This is common but means DNS responses for 2 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].cloudfront.net: 1 hostname
  - INFO **DNSSEC is not configured**: Zone [redacted].cloudfront.net has no DNSSEC configured (no DS record in parent zone cloudfront.net). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].airbus.com: 1 hostname
  - INFO **DNSSEC is not configured**: Zone [redacted].airbus.com has no DNSSEC configured (no DS record in parent zone airbus.com). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].airbus.com: 1 hostname
  - INFO **DNSSEC is not configured**: Zone [redacted].airbus.com has no DNSSEC configured (no DS record in parent zone airbus.com). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].akamaiedge.net: 5 hostnames
  - INFO **DNSSEC is not configured**: Zone [redacted].akamaiedge.net has no DNSSEC configured (no DS record in parent zone akamaiedge.net). This is common but means DNS responses for 5 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].akamaiedge.net: 2 hostnames
  - INFO **DNSSEC is not configured**: Zone [redacted].akamaiedge.net has no DNSSEC configured (no DS record in parent zone akamaiedge.net). This is common but means DNS responses for 2 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].cloudfront.net: 1 hostname
  - INFO **DNSSEC is not configured**: Zone [redacted].cloudfront.net has no DNSSEC configured (no DS record in parent zone cloudfront.net). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].airbus.com: 1 hostname
  - INFO **DNSSEC is not configured**: Zone [redacted].airbus.com has no DNSSEC configured (no DS record in parent zone airbus.com). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].[redacted].[redacted].cloud: 1 hostname
  - INFO **DNSSEC is not configured**: Zone [redacted].[redacted].[redacted].cloud has no DNSSEC configured (no DS record in parent zone [redacted].[redacted].cloud). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].[redacted].[redacted].cloud: 9 hostnames
  - INFO **DNSSEC is not configured**: Zone [redacted].[redacted].[redacted].cloud has no DNSSEC configured (no DS record in parent zone [redacted].[redacted].cloud). This is common but means DNS responses for 9 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].[redacted].[redacted].cloud: 1 hostname

- INFO **DNSSEC is not configured**: Zone [redacted].cloud has no DNSSEC configured (no DS record in parent zone [redacted].cloud). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.

- INSECURE **edgekey.net**: 1 hostname
  - INFO **DNSSEC is not configured**: Zone edgekey.net has no DNSSEC configured (no DS record in parent zone net). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].**amazonaws.com**: 1 hostname
  - INFO **DNSSEC is not configured**: Zone [redacted].amazonaws.com has no DNSSEC configured (no DS record in parent zone [redacted].amazonaws.com). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].**amazonaws.com**: 1 hostname
  - INFO **DNSSEC is not configured**: Zone [redacted].amazonaws.com has no DNSSEC configured (no DS record in parent zone [redacted].amazonaws.com). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].**airbus.com**: 2 hostnames
  - INFO **DNSSEC is not configured**: Zone [redacted].airbus.com has no DNSSEC configured (no DS record in parent zone airbus.com). This is common but means DNS responses for 2 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- SECURE [redacted].**com**: 1 hostname
  - Algorithm: ECDSAP256SHA256
  - NSEC mode: nsec3
  - Earliest sampled signature expiry: 2026-11-19T00:00:00Z (13 days)
  - GOOD **DNSSEC is properly configured with modern cryptography**: Zone [redacted].com is DNSSEC-secured with ECDSAP256SHA256 (algorithm 13), NSEC3 denial of existence, and SHA-256+ DS digest. Sampled signatures are valid for at least 13 more days. 1 scanned hostnames are protected by this zone's DNSSEC configuration.
- INSECURE [redacted].**com.cn**: 1 hostname
  - INFO **DNSSEC is not configured**: Zone [redacted].com.cn has no DNSSEC configured (no DS record in parent zone [redacted].com.cn). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- ERROR [redacted].**azure.com**: 1 hostname
- INSECURE [redacted].**cloud**: 1 hostname
  - INFO **DNSSEC is not configured**: Zone [redacted].cloud has no DNSSEC configured (no DS record in parent zone [redacted].cloud). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE **googlehosted.com**: 12 hostnames
  - INFO **DNSSEC is not configured**: Zone googlehosted.com has no DNSSEC configured (no DS record in parent zone com). This is common but means DNS responses for 12 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- SECURE [redacted].**net**: 2 hostnames
  - Algorithm: ECDSAP256SHA256
  - Earliest sampled signature expiry: 2026-11-06T06:35:17Z (1 days)

- GOOD **DNSSEC is configured and functional**: Zone [redacted].net is DNSSEC-secured with ECDSAP256SHA256 (algorithm 13). The configuration is functional. See informational findings for upgrade recommendations.

- SECURE **[redacted].net**: 1 hostname
  - Algorithm: ECDSAP256SHA256
  - NSEC mode: nsec-black-lies
  - Earliest sampled signature expiry: 2026-11-06T06:35:17Z (1 days)
  - GOOD **DNSSEC is configured and functional**: Zone [redacted].net is DNSSEC-secured with ECDSAP256SHA256 (algorithm 13). The configuration is functional. See informational findings for upgrade recommendations.
- SECURE **impervadns.net**: 300 hostnames
  - Algorithm: RSASHA256
  - NSEC mode: nsec3
  - Earliest sampled signature expiry: 2027-01-06T00:00:00Z (61 days)
  - WARNING **RSA key size is too small**: Zone impervadns.net uses a 1024-bit RSA ZSK (key tag 11304). Keys under 2048 bits are considered factorable with sufficient resources. Upgrade to 2048-bit minimum or migrate to ECDSA.
  - INFO **Stronger signing algorithm available**: Zone impervadns.net is signed with RSASHA256 (algorithm 8), which is functional but not optimal. ECDSAP256SHA256 (algorithm 13) provides equivalent security with smaller signatures and better performance. Consider migrating.
  - GOOD **DNSSEC is configured and functional**: Zone impervadns.net is DNSSEC-secured with RSASHA256 (algorithm 8). The configuration is functional. See informational findings for upgrade recommendations.
- INSECURE [redacted].[redacted].cloud: 2 hostnames
  - INFO **DNSSEC is not configured**: Zone [redacted].[redacted].cloud has no DNSSEC configured (no DS record in parent zone [redacted].cloud). This is common but means DNS responses for 2 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].com: 2 hostnames
  - INFO **DNSSEC is not configured**: Zone [redacted].com has no DNSSEC configured (no DS record in parent zone com). This is common but means DNS responses for 2 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].eu: 6 hostnames
  - INFO **DNSSEC is not configured**: Zone [redacted].eu has no DNSSEC configured (no DS record in parent zone eu). This is common but means DNS responses for 6 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].airbus.com: 11 hostnames
  - INFO **DNSSEC is not configured**: Zone [redacted].airbus.com has no DNSSEC configured (no DS record in parent zone airbus.com). This is common but means DNS responses for 11 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].[redacted].[redacted].net: 1 hostname
  - INFO **DNSSEC is not configured**: Zone [redacted].[redacted].[redacted].net has no DNSSEC configured (no DS record in parent zone [redacted].[redacted].net). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].airbus.com: 3 hostnames
  - INFO **DNSSEC is not configured**: Zone [redacted].airbus.com has no DNSSEC configured (no DS record in parent zone airbus.com). This is common but means DNS responses for 3

hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.

- INSECURE [redacted].[redacted].[redacted].**cloud**: 15 hostnames
  - INFO **DNSSEC is not configured**: Zone [redacted].[redacted].[redacted].cloud has no DNSSEC configured (no DS record in parent zone [redacted].[redacted].cloud). This is common but means DNS responses for 15 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].**airbus.com**: 222 hostnames
  - INFO **DNSSEC is not configured**: Zone [redacted].airbus.com has no DNSSEC configured (no DS record in parent zone airbus.com). This is common but means DNS responses for 222 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].**com**: 1 hostname
  - INFO **DNSSEC is not configured**: Zone [redacted].com has no DNSSEC configured (no DS record in parent zone com). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- SECURE [redacted].**com**: 1 hostname
  - Algorithm: ECDSAP256SHA256
  - Earliest sampled signature expiry: 2026-11-06T06:35:17Z (1 days)
  - GOOD **DNSSEC is configured and functional**: Zone [redacted].com is DNSSEC-secured with ECDSAP256SHA256 (algorithm 13). The configuration is functional. See informational findings for upgrade recommendations.
- INSECURE [redacted].**airbus.com**: 5 hostnames
  - INFO **DNSSEC is not configured**: Zone [redacted].airbus.com has no DNSSEC configured (no DS record in parent zone airbus.com). This is common but means DNS responses for 5 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].**com**: 1 hostname
  - INFO **DNSSEC is not configured**: Zone [redacted].com has no DNSSEC configured (no DS record in parent zone com). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].**airbus.com**: 1 hostname
  - INFO **DNSSEC is not configured**: Zone [redacted].airbus.com has no DNSSEC configured (no DS record in parent zone airbus.com). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].**airbus.com**: 3 hostnames
  - INFO **DNSSEC is not configured**: Zone [redacted].airbus.com has no DNSSEC configured (no DS record in parent zone airbus.com). This is common but means DNS responses for 3 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].**airbus.com**: 3 hostnames
  - INFO **DNSSEC is not configured**: Zone [redacted].airbus.com has no DNSSEC configured (no DS record in parent zone airbus.com). This is common but means DNS responses for 3 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].**fr**: 1 hostname
  - INFO **DNSSEC is not configured**: Zone [redacted].fr has no DNSSEC configured (no DS record in parent zone fr). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- INSECURE [redacted].[redacted].**com**: 2 hostnames

- INFO **DNSSEC is not configured**: Zone [redacted].[redacted].com has no DNSSEC configured (no DS record in parent zone [redacted].com). This is common but means DNS responses for 2 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.

- INSECURE **web.app**: 1 hostname
  - INFO **DNSSEC is not configured**: Zone web.app has no DNSSEC configured (no DS record in parent zone app). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.
- SECURE **[redacted].com**: 5 hostnames
  - Algorithm: ECDSAP256SHA256
  - Earliest sampled signature expiry: 2026-11-06T06:35:17Z (1 days)
  - GOOD **DNSSEC is configured and functional**: Zone [redacted].com is DNSSEC-secured with ECDSAP256SHA256 (algorithm 13). The configuration is functional. See informational findings for upgrade recommendations.
- ERROR **[redacted].incapdns.net**: 33 hostnames
- INSECURE **[redacted].eu**: 1 hostname
  - INFO **DNSSEC is not configured**: Zone [redacted].eu has no DNSSEC configured (no DS record in parent zone eu). This is common but means DNS responses for 1 hostnames in this zone cannot be authenticated. Consider enabling DNSSEC, especially for zones serving security-sensitive services.

Unresolvable hostnames

- NXDOMAIN: 386 hostnames. Examples: [redacted].airbus.com, [redacted].airbus.com, [redacted].airbus.com. Full inventory is available in the interactive report.

10 Email Security

This section reviews receiving mail routes, SMTP transport encryption, certificates, and domain-level mail policies for the submitted domain.

Mail overview

- Checked domain: airbus.com
- Mail acceptance: Mail service found through MX records
- MX hosts: 2
- Attempted endpoints: 6
- Reachable port 25 delivery endpoints: 2
- Submission endpoints observed: 0
- Scan duration: 9.7 seconds
- Truncated: no

↓ Download mx details (CSV)
↓ Download smtp details (CSV)
↓ Download policies details (CSV)
↓ Download findings details (CSV)

MX and SMTP transport

A missing listener on port 465 or 587 does not prove that the domain lacks a separate submission service. MX records identify delivery hosts, not every hostname used by mail clients.

[redacted].[redacted].net Priority 4; 3 attempted endpoints 1 delivery endpoints checked; 1 reported reachable. Complete transport, certificate, and greeting evidence is in the SMTP CSV.

- [redacted]:25: delivery; listener listening; starttls success; TLS TLS1.2, TLS1.3.
- [redacted]:465: submission; listener filtered; implicit_tls not_attempted; TLS not observed.

1 additional endpoint results are available in the SMTP CSV.

[redacted].[redacted].net Priority 8; 3 attempted endpoints 1 delivery endpoints checked; 1 reported reachable. Complete transport, certificate, and greeting evidence is in the SMTP CSV.

- [redacted]:25: delivery; listener listening; starttls success; TLS TLS1.2, TLS1.3.
- [redacted]:465: submission; listener filtered; implicit_tls not_attempted; TLS not observed.

1 additional endpoint results are available in the SMTP CSV.

Authentication and transport policies

- **SPF**: present; fail; Syntax valid; alignment Not applicable; reports none; MX Not applicable; DANE and DNSSEC Not applicable; issues none
- **DMARC**: present; reject; Record parsed; alignment DKIM default; SPF default; reports mailto:[redacted]@[redacted].com, mailto:[redacted]@airbus.com, mailto:[redacted]@airbus.com; MX Not applicable; DANE and DNSSEC Not applicable; issues none
- **MTA-STS**: absent; Not determined; not_attempted; Not reported; alignment Not applicable; reports none; MX Not reported; DANE and DNSSEC Not applicable; issues none
- **TLS-RPT**: absent; Not enabled; absent; alignment Not applicable; reports none; MX Not applicable; DANE and DNSSEC Not applicable; issues none
- **DANE**: absent; TLSA certificate association; 0 matching TLSA records; alignment Not applicable; reports none; MX 2 MX hosts checked on port 25; DANE and DNSSEC insecure; issues none

Grouped findings

- **airbus.com**: 1 informational findings in MTA-STS; 0 affected endpoints
  - **MTA-STS is not published**: No MTA-STS policy was discovered. (MTA_STS_ABSENT; 1 occurrences)
- **airbus.com**: 1 informational findings in TLS-RPT; 0 affected endpoints
  - **TLS-RPT is not published**: No SMTP TLS reporting policy was discovered. (TLS_RPT_ABSENT; 1 occurrences)

Operational diagnostics

Probe and DNS errors are listed separately from security findings.

- **TIMEOUT**: 4 probe results from SMTP endpoint. dial tcp [redacted]:465: i/o timeout Examples: [redacted].net [redacted]:465, [redacted].net [redacted]:587.

The interactive report contains the complete operational diagnostics.

11 Adjacent Domains

These off-scope SANs were observed on the same certificates but belong to other apex domains.
↓ Download adjacent domains (CSV)

APEX DOMAIN	SANS
[redacted].com	175
[redacted].cloud	53
[redacted].com	21
[redacted].com	12

Showing 4 of 192 domains. Download the CSV for the full list.