

SERVICIUL
TEHNOLOGIA INFORMAȚIEI
ȘI SECURITATE CIBERNETICĂ

RAPORT TEHNIC DE SECURITATE

GoAhead
Validarea certificatelor
și securitatea TLS

1 Sumar executiv

Se recomandă inventarierea dispozitivelor care includ GoAhead și aplicarea unui firmware care integrează GoAhead 6.1.1 sau o corecție echivalentă confirmată de producător. Prioritatea operațională revine interfețelor de administrare expuse și instalațiilor care folosesc certificate client pentru controlul accesului. Actualizarea bibliotecii TLS, singură, nu corectează codul de integrare GoAhead.

GoAhead este un server web integrat în dispozitive. Autentificarea TLS mutuală (mTLS) verifică identitatea clientului prin certificat; CRL este lista certificatelor revocate. Tema principală este neaplicarea verificării revocării în integrarea compatibilă OpenSSL. Sunt analizate separat și depășirea limitei lanțului în anumite builduri LibreSSL, respectiv parametrii Diffie–Hellman incorecți din integrarea Mbed TLS. Funcțiile compilate, biblioteca și politica de verificare determină expunerea.

Problemă	Scor EmbedThis	Condiție esențială	Corectat în
CVE-2026-115881 CRL neaplicată	9,1 Critic	OpenSSL compatibil, mTLS și CRL configurate.	6.1.1
CVE-2026-115884 Limită de lanț ocolită	7,4 Ridicat	LibreSSL legacy, certificat client cerut și verificarea emitentului oprită.	6.1.1
GHSA-fmvx-2xfx-2gq4 Parametri DH trunchiați	5,9 Moderat	Mbed TLS, DHE_RSA și client care acceptă grupul defect.	6.1.1

Concluzii pentru decizia de remediere

- Acceptarea unui certificat revocat nu presupune acces anonim cu orice certificat. Se verifică identitatea anterior autorizată, posesia cheii private și accesul la endpointul protejat. Drepturile finale depind de autorizarea aplicației.
- Nu se atribuie automat vulnerabilitatea unui producător sau unei familii de echipamente doar pentru că utilizează GoAhead. Sunt necesare modelul, firmware-ul, backendul TLS și configurația reală.
- Se confirmă atât instalarea corecției, cât și respingerea certificatului revocat într-un handshake complet nou. Existența fișierului CRL sau absența erorilor la pornire nu sunt dovezi suficiente.

2 Fișa tehnică pentru verificarea revocării

CVE-2026-115881 | GOAHEAD-SA-2026-0006 | GHSA-5m75-xq69-c3c5

Câmp tehnic	Evaluare
Descriere succintă	O CRL configurată este încărcată, dar verificarea revocării nu este activată. Un certificat client revocat poate fi acceptat.
Componentă și cauză	src/openssl.c, sslOpen(); lipsește activarea X509_V_FLAG_CRL_CHECK după încărcarea CRL.
Versiuni afectate	GoAhead 3.4.5–6.1.0, cu backend compatibil OpenSSL și configurația relevantă. Remediat upstream în 6.1.1.
Configurație relevantă	ME_COM_OPENSSL=1; ME_GOAHEAD_SSL_VERIFY_PEER=1; ME_GOAHEAD_SSL_AUTHORITY și ME_GOAHEAD_SSL_REVOKE configurate; în scenariul de încredere strictă, ME_GOAHEAD_SSL_VERIFY_ISSUER=1.
Condiții pentru atacator	Acces la serviciu și un certificat client anterior de încredere, înscris în CRL. Autentificarea TLS presupune și posesia cheii private corespunzătoare.
Tipul vulnerabilității	CWE-299 — verificarea incorectă a revocării; CWE-295 — validarea incorectă a certificatului.

Câmp tehnic	Evaluare
Consecințe	Identitatea revocată poate păstra accesul pe care aplicația îl acordă certificatului. Nu este demonstrată prin acest defect executare de cod directă.
Configurații distincte	Buildurile Mbed TLS au altă cale de verificare CRL. Configurația implicită GoAhead nu activează mTLS și CRL.
Detectare recomandată	Corelarea emitentului și serialului certificatului cu CRL efectiv încărcată, momentul revocării, handshake-ul și operațiile ulterioare.

3 Mecanismul și limita corecției CRL

Încărcarea unei liste și aplicarea ei sunt pași separați

Analiza surselor 6.1.0 și 6.1.1 arată modificarea în sslOpen(). Fișierul poate fi încărcat cu succes fără activarea verificării revocării. Versiunea corectată setează flagul pe depozitul de certificate imediat după încărcare.

```
X509_STORE_set_flags(store, X509_V_FLAG_CRL_CHECK);
```

Etapă	Ce trebuie să se întâmple	Dovadă urmărită
Configurație și încărcare	Serviciul identifică CA și CRL folosite pentru certificatul client.	Fișierul corect, emitentul, integritatea și data actualizării.
Verificare X509	Politica activează consultarea CRL pentru certificatul vizat.	Comportamentul real al verificatorului, nu doar existența fișierului.
Respingere	Certificatul final revocat este refuzat de verificare.	Eroare de revocare ori cod echivalent documentat; conexiunea nu obține acces.
Autorizare aplicație	Identitatea validată primește doar drepturile aprobate.	Corelare între identitatea certificatului, sesiune și resursa accesată.

Verificarea certificatului final

Documentația OpenSSL precizează că X509_V_FLAG_CRL_CHECK verifică certificatul final, numit leaf. Verificarea întregului lanț necesită și CRL_CHECK_ALL, iar absența unei CRL potrivite produce eroare când verificarea este cerută. Corecția GoAhead activează verificarea leaf; nu demonstrează automat o politică de revocare pentru toate CA intermediare.

Dacă instituția cere verificare pe întregul lanț, cerința se stabilește separat cu furnizorul: liste necesare, actualizare, tratamentul erorilor și teste. Nu se modifică firmware-ul nesuportat numai prin adăugarea unui flag în sursele de referință.

Ce nu stabilește o verificare izolată

- Un rezultat OpenSSL din terminal descrie acea comandă și acele fișiere. Nu dovedește ce bibliotecă, configurație sau CRL folosește procesul GoAhead din dispozitiv.
- Un certificat revocat, dar expirat sau cu emitent neacceptat, poate fi respins din alt motiv. Pentru regresie se folosește un certificat altfel valid și se păstrează motivul exact al respingerii.
- Conexiunile existente și reluarea sesiunilor trebuie evaluate separat de un handshake nou. Se consemnează dacă testul a folosit sesiune completă ori reluată.

4 Fișa tehnică pentru limita lanțului

CVE-2026-115884 | GOAHEAD-SA-2026-0004 | GHSA-r392-vqwx-3r4g

Câmp tehnic	Evaluare
Descriere și efect	O limită de adâncime a lanțului client poate fi ocolită pe anumite builduri LibreSSL.
Versiuni GoAhead	≤ 6.1.0; remediat upstream în 6.1.1.
Bibliotecă relevantă	Verificatorul legacy din LibreSSL 3.2.x sau 3.3.2–3.3.6.
Configurație necesară	ME_GOAHEAD_SSL_VERIFY_PEER=1 și ME_GOAHEAD_SSL_VERIFY_ISSUER=0.
Acces pentru atacator	Acces HTTPS și lanț controlat de atacator peste limita configurată, implicit VERIFY_DEPTH=10. Nu este necesar material criptografic de încredere.
Cauză	Controlul adâncimii putea fi omis în prezența unei erori anterioare, iar configurația tolera eroarea privind emitentul local necunoscut.
Tipul vulnerabilității	CWE-287, CWE-295 și CWE-754, conform metadatelor avizului.
Limite ale domeniului	Scenariul descris nu afectează OpenSSL, BoringSSL, AWS-LC, LibreSSL 4.x sau calea Mbed TLS.
Mecanism de remediere	GoAhead verifică necondiționat adâncimea înainte de acceptarea specifică unui cod de eroare.

Interpretarea riscului

Când verificarea emitentului este oprită, certificatul autosemnat obișnuit poate fi deja permis de politică. Defectul analizat ocolește suplimentar limita lanțului. Această distincție este necesară pentru a nu confunda problema cu ocolirea unei politici care cere o CA de încredere.

Control temporar și validare

Avizul indică activarea verificării emitentului cu un set CA de încredere ori utilizarea unui backend neafectat de acest mecanism. În GoAhead, opțiunile pot fi stabilite la compilare. Implementarea se face prin mecanismul permis de producător, cu testarea clienților legitimi și a lanțurilor excesive. O schimbare de backend se reevaluează și pentru defectul CRL.

5 Fișa tehnică pentru parametrii Diffie Hellman

GOAHEAD-SA-2026-0005 | GHSA-fmvx-2xfx-2gq4

Câmp tehnic	Evaluare
Identificator	Avizul GHSA nu indică un CVE la data consultării. Referința principală rămâne GHSA-fmvx-2xfx-2gq4.
Domeniu afectat	GoAhead 4.0.2–6.1.0 cu backend Mbed TLS; remediat în 6.1.1.
Condiții necesare	DHE_RSA în TLS 1.2 ori anterior, client care acceptă parametrii defecți și observarea traficului de către atacator.
Cauză în integrare	Lungimea modulului DH este preluată greșit din bufferul generatorului. În sursa corectată se utilizează sizeof(dhm_p).
Consecință	Un modul de un octet, P=255, înlocuiește grupul de 2048 biți. Sesiunea completată de un client permisiv poate fi decriptată de un observator pasiv.
Tipul vulnerabilității	CWE-327, CWE-682 și CWE-1240, conform metadatelor avizului.
Domeniu neafectat de acest defect	TLS 1.3, ECDHE și implementarea GoAhead cu OpenSSL. Refuzul parametrilor de către client poate împiedica realizarea sesiunii vulnerabile.

Suite relevante pentru triere

Cod IANA	Denumire corectă
0x009E	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
0x009F	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
0xCCAA	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256

Denumirile sunt verificate în registrul IANA. O suită DHE observată este un indiciu de verificat, nu dovada unui modul trunchiat. Se confirmă backendul și parametrii handshake-ului, în condiții de colectare aprobate.

6 Inventarierea dispozitivelor și a buildurilor

Prezența unui banner GoAhead sau a unei amprente TLS inițiază evaluarea. Clasificarea necesită confirmarea componentelor din firmware, a opțiunilor compilate și a politicii efectiv aplicate. Un model menționat generic în presă nu este declarat automat afectat.

Câmp de inventar	Informație necesară
Dispozitiv și rol	Model, revizie hardware, identificator intern, funcție și responsabil.
Firmware	Versiune completă, data instalării, hash sau semnătură și mecanism de actualizare.
GoAhead și biblioteca TLS	Versiune, backend, versiunea bibliotecii și confirmare SBOM ori document al furnizorului.
Politica de certificate	VERIFY_PEER, VERIFY_ISSUER, CA de încredere, CRL folosită, limita lanțului și locul terminării TLS.
Protocoale și suite	TLS negociat, DHE_RSA versus ECDHE și comportamentul clienților integrați.
Acoperirea corecției	Versiune remediată sau backport confirmat pentru model, dovezi și rezultat de validare.

Amprente JA4Scan publicate pentru triere

Build de referință	JA4Scan TLS pentru GoAhead din seria 6.1
OpenSSL 3.6.2	03100h0s00sn_1fe27f6025fb_d06dc4648d2f_sr00ss537461
LibreSSL 3.3.6	03100h0s00s0_9d52559f55bc_c64486648d2f_sr00sc24603c
LibreSSL 4.3.1	03100h0r00s0_9d52559f55bc_c64486206461_sr00scc98ba1
Mbed TLS 3.6.6	23100h0s01s0_d7d3025021f4_0475c5cede0d_sr0ss02265cf

Valorile sunt cele publicate de FoxIO. Nu sunt IOC-uri de atac și nu separă automat un firmware remediat de unul vulnerabil. JA4Scan este o metodă activă; eventuala folosire se limitează la active autorizate și la o fereastră potrivită pentru dispozitivele operaționale.

Verificarea configurației compilate

Documentația GoAhead descrie cerința de certificat client, setul CA și verificarea emitentului ca opțiuni de configurare a serviciului. În produsele integrate, confirmarea se obține din informația de build sau de la producător. Un panou web care afișează mTLS activ nu demonstrează singur aplicarea revocării.

7 Detectare și verificări locale

Semnal	Date de corelat	Interpretare
Certificat revocat acceptat	Emitent, serial, CRL activă, ora handshake-ului, identitate și resursă accesată.	Indiciu direct al neaplicării revocării, dacă certificatul și lista sunt cele folosite efectiv.
Lanț peste limita configurată acceptat	Biblioteca, opțiunile de emitent, adâncimea, codul verificatorului și răspunsul aplicației.	Posibilă cale LibreSSL; se exclud alte politici care permit explicit acel client.
TLS cu DHE_RSA	Backend, client, cod de suită și parametrii DH disponibili în telemetrie.	Necesită analiză suplimentară; alegerea DHE nu dovedește singură slăbiciunea.
Acces de la un dispozitiv retras	Inventar, momentul retragerii și revocării, sesiuni active și operații de administrare.	Posibilă folosire a unei identități care trebuia blocată; se stabilește legitimitatea accesului.

Analiza offline a certificatului și a CRL

Exemplele folosesc fișiere locale și nu necesită cheia privată a clientului. Se adaptează numele la materialele de test sau la copiile autorizate. Sintaxa este documentată de OpenSSL.

```
openssl x509 -in client.pem -noout \
  -issuer -serial -dates -fingerprint -sha256

openssl crl -in crl.pem -noout \
  -issuer -lastupdate -nextupdate -fingerprint -sha256

openssl crl -in crl.pem -noout -verify -CAfile ca.pem

openssl verify -purpose sslclient -CAfile ca.pem \
  -CRLfile crl.pem -crl_check client.pem
```

Pentru un lanț cu intermediare se adaugă -untrusted intermediates.pem, dacă este necesar. Verificarea semnăturii CRL nu certifică utilizarea ei de GoAhead. Comanda verify verifică acel certificat cu acele fișiere și opțiuni; rezultatul nu înlocuiește testul pe endpointul care protejează serviciul.

Limitele telemetriei

Se păstrează metadatele necesare fără exportul cheilor private. Înaintea unei concluzii negative se verifică retenția, vizibilitatea TLS și locul unde se termină conexiunea. Un timeout, o eroare de rețea sau lipsa alertelor nu demonstrează respingerea corectă a certificatului.

8 Validarea remedierii

Matricea de mai jos este un plan de acceptare propus. Testele cu certificate și clienți dedicați se efectuează într-un laborator sau printr-o procedură aprobată pentru dispozitiv. Nu se folosesc în raport certificate private ori interfețe ale beneficiarului.

Test	Condiție de control	Rezultat urmărit
Client legitim	Certificat în termen, CA aprobată, nerevocat, drepturi cunoscute.	Accesul legitim funcționează conform politicii aplicației.
Client revocat	Certificat altfel valid, înscris în CRL activă; handshake complet nou.	Revocarea este motivul respingerii; nu se obține acces. Se păstrează codul verificatorului.
Emitent neacceptat	Verificarea emitentului este cerută de politică.	Lanțul neautorizat este respins. Nu se substituie cu succesul altui test de revocare.
Certificat expirat sau absent	mTLS cerut; ceas corect și test separat pentru fiecare situație.	Certificatul expirat și lipsa certificatului nu acordă acces.
CRL lipsă sau expirată	Politica de funcționare la eroare este stabilită și documentată.	Serviciul nu permite accesul fără verificarea cerută; erorile sunt observabile.
Lanț excesiv	Configurația și limita lanțului sunt confirmate; material de test dedicat.	Depășirea este respinsă indiferent de o altă eroare de validare tolerată.
Parametri DHE	Cale Mbed TLS testată în laborator; analiză a parametrilor ori DHE dezactivat.	Grupul configurat corect este transmis sau negocierea DHE este imposibilă prin politica aprobată.
Sesiuni și redundanță	Se diferențiază handshake complet, reluare, conexiuni existente și noduri.	Politica rămâne coerentă după invalidarea sesiunilor și comutarea pe nodul de rezervă.

9 Contextul versiunii și răspunsul la incident

Cele unsprezece avize remediate

Contextul de mai jos explică de ce actualizarea trebuie evaluată pentru întregul dispozitiv. Este o sinteză a notelor EmbedThis; fișele detaliate ale raportului rămân concentrate asupra celor trei defecte TLS. Toate avizele din tabel sunt declarate rezolvate în 6.1.1.

Aviz din 2026	Severitate	Domeniu
0001	Critic	Ocolire Basic și formular pentru parole BF1.
0002	Moderat	Divulgarea secretului serverului prin nonce Digest.
0003	Ridicat	Mediu CGI și HTTP_PROXY.
0004	Ridicat	Limită de lanț mTLS în anumite builduri LibreSSL.
0005	Moderat	Trunchierea parametrilor DH în Mbed TLS.
0006	Critic	CRL neaplicată în integrarea OpenSSL.
0007	Critic	Injecție de comenzi CGI pe Windows.
0008	Moderat	Request smuggling prin Content Length și Transfer Encoding.
0009	Ridicat condiționat	Injecție de argumente și opțiuni CGI ISINDEX.
0010	Moderat	Request smuggling prin HEAD și dimensiuni chunked.
0011	Scăzut	Fixarea identificatorului sesiunii.

Prefixul complet al identificatorilor este GOAHEAD-SA-2026-. Notele versiunii recomandă și rotația parolelor BF1, unde sunt folosite. GoAhead se află în etapa de mentenanță, cu actualizări de securitate în continuare.

Investigarea unui acces după revocare

Dacă sunt găsite conexiuni de la o identitate revocată, se verifică momentul revocării, versiunea CRL folosită la acel moment, existența unei sesiuni anterioare și operațiile efectuate. Se păstrează jurnalele și configurația înaintea curățării. Se limitează calea expusă și se evaluează datele și secretele la care identitatea avea acces.

Pentru o posibilă divulgare prin DHE se analizează ce trafic a traversat sesiunile relevante. Se înlocuiesc credențialele sau tokenurile posibil expuse, potrivit dovezilor și impactului. Actualizarea nu elimină copii ale traficului deja înregistrat. Acestea sunt recomandări de răspuns, nu constatări de compromitere locală.

10 Surse și limite metodologice

Surse consultate la 28 octombrie 2026. Identificatorii, scorurile CVSS și intervalele provin din avizele EmbedThis. Codul sursă 6.1.0 și 6.1.1 susține analiza mecanismelor. Pașii de inventariere, detectare și acceptare sunt recomandări operaționale ale raportului.

Cyber Kendra — Articolul tematic despre certificatele mTLS revocate

FoxIO — Choose Your Backend Three TLS Bugs in GoAhead

EmbedThis — GOAHEAD SA 2026 0006 CRL neaplicată

EmbedThis — GOAHEAD SA 2026 0004 Limită de lanț mTLS

EmbedThis — GOAHEAD SA 2026 0005 Parametri Mbed TLS DH

EmbedThis — GoAhead 6.1.1 și notele de migrare

Cod sursă GoAhead — openssl.c în 6.1.0

Cod sursă GoAhead — openssl.c în 6.1.1

Cod sursă GoAhead — mbedtls.c în 6.1.0

Cod sursă GoAhead — mbedtls.c în 6.1.1

OpenSSL — X509 VERIFY PARAM și flagurile de verificare

OpenSSL — Opțiunile verificării certificatelor

OpenSSL — Comanda verify

OpenSSL — Comanda crl

OpenSSL — Comanda x509

IANA — Registrul TLS Cipher Suites

EmbedThis — Documentația SSL pentru GoAhead

Limite: nu sunt disponibile configurații ori rezultate de verificare locale pentru stabilirea activelor afectate. Menționarea unui backend, a unui banner sau a unei amprente nu constituie confirmarea vulnerabilității unui dispozitiv. Închiderea necesită o corecție confirmată pentru model și dovezi locale de funcționare a politicii cerute.