GRILLI

PENETRATION TEST REPORT

Offensive Security Assessment

Penetration Test Report

3DS Environment (3DE) — Offensive Security Assessment

Document Control

Report reference	GS-PT-2026-0483
Report title	3DS Environment (3DE) Penetration Test — PayNova
Client	the Client (anonymized)
Assessment type	Grey-box penetration test of the EMV 3-D Secure environment (3DE)
Scope (summary)	EMV 3-D Secure Server (3DSS) and integration endpoints (3ds.paynova.example)
Testing window	1 June 2026 – 5 June 2026 (5 business days)
Report date (initial issue)	7 June 2026
Final issue (incl. retest)	16 June 2026
Remediation completed	14 June 2026
Retest date	15 June 2026 (24h after remediation)
Document version	1.0 (Final)
Classification	CONFIDENTIAL
Prepared by	Grilli Security — lime@grillisecurity.com

Version History

Version	Date	Author	Notes
0.1	6 June 2026	Lead Consultant	Internal draft
0.9	7 June 2026	Technical Reviewer (QA)	Report delivered (pre-retest) / QA
1.0	16 June 2026	Grilli Security	Final issue incl. retest results

Distribution

This document is classified CONFIDENTIAL and is restricted to the named recipients within the Client organization and their authorized assessors and regulators (e.g. acquiring bank / QSA, where applicable). It must not be redistributed without written consent.

Anonymization note. *This is a sample report. The client name, the platform name ("PayNova"), all hostnames (example domains), IP addresses (RFC 5737 documentation ranges) and evidence have been anonymized or redacted. No real data is contained herein.*

Attestation & Statement of Independence

Grilli Security attests that the penetration test described in this report was performed in accordance with the methodology stated herein (EMVCo 3DS; PCI 3DS Core; NIST SP 800-115) by qualified, suitably-certified personnel, and that the assessment team maintained organizational independence from the development and operation of the systems under test, consistent with PCI DSS v4.0 Requirement 11.4.1 (penetration-testing methodology, qualified resources and tester independence).
The findings, severity ratings and conclusions represent the independent professional opinion of the assessment team based on the evidence gathered during the testing window. This attestation supports the Client's PCI DSS Req 11.4 and DORA (Art. 24–25) assurance obligations.

Sign-off

Role	Name / Reference	Date
Lead Penetration Tester	[Anonymized] — OSCP, OSWE, CREST CRT	15 Jun 2026
Technical Reviewer / QA	[Anonymized] — CREST CCT App, OSCP	16 Jun 2026
Authorized by (Grilli Security)	[Anonymized] — Head of Offensive Security	16 Jun 2026

Signatures are held on file in the secure project record; names are anonymized in this sample. Sign-off dates are on or before the final-issue date (16 June 2026).

Table of Contents

1. Executive Summary

1.1 Overview

Grilli Security performed a grey-box penetration test of the PayNova EMV 3-D Secure environment (3DE), covering the 3DS Server (3DSS) and its integration endpoints at 3ds.paynova.example. The 3DE boundary comprises the 3DSS, its message-intake endpoints and the 3DS Method browser flow. Testing was conducted between 1 June 2026 and 5 June 2026, following the EMVCo EMV 3-D Secure Specification, the PCI 3DS Core Security Standard and NIST SP 800-115, with findings scored using CVSS v4.0.
The assessment identified a critical authentication-result integrity bypass — the 3DS Server accepted a forged, unsigned ARes — alongside sensitive-data exposure and integration weaknesses. In total, 6 findings were raised.

1.2 Overall Risk Rating

At the time of testing the overall risk was assessed as **CRITICAL**. Following the engagement, the Client remediated all findings; an independent retest (15 June 2026, 24 hours after remediation) confirmed every issue as closed. The post-remediation residual risk is assessed as **LOW**.

1.3 Summary of Findings

Severity	Count	Description
Critical	**1**	Immediate, business-critical exposure or full compromise.
High	**2**	Serious weakness materially increasing breach likelihood or impact.
Medium	**3**	Notable hardening gap to be remediated in the normal cycle.
Low	**0**	Lower-risk best-practice item.
Informational	**0**	Observational; no direct risk.

Total findings: **6** | Status: all remediated and verified at retest.

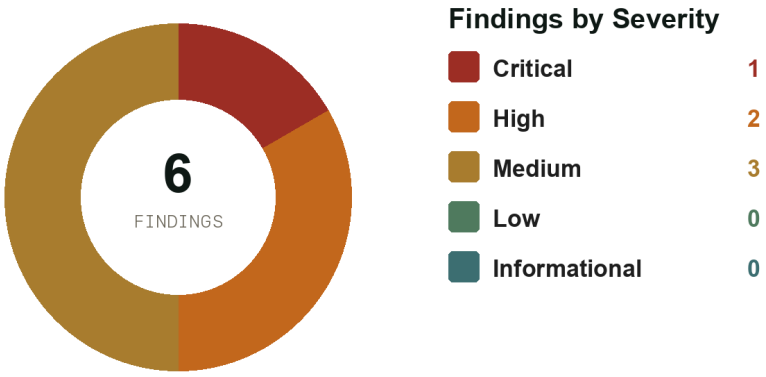

Figure 1 — Findings by severity (n = 6).

Note. *Severity reflects the CVSS v4.0 base-score band, refined by the payment-authentication sensitivity of the 3DE.*

1.4 Key Risks

- Authentication-result integrity could be bypassed (D-01): the 3DSS accepted a forged/unsigned ARes indicating success, defeating the core fraud-prevention purpose of 3-D Secure.

- Authentication results could be replayed (D-04): missing nonce/transaction binding allowed a valid result to authorize a different transaction.
- Sensitive authentication values were exposed (D-02): CAVV was returned to the merchant and written to logs.
- The browser integration trusted cross-origin messages (D-03): 3DS Method postMessage origins were not validated.

1.5 Strategic Recommendations

- Enforce cryptographic validation of every 3-D Secure message (ARes/CRes) and bind each to a single-use transaction nonce.
- Treat CAVV and authentication values as sensitive: never log them and minimize their exposure in responses.
- Harden the browser integration (postMessage origin validation, CSP) and the transport (modern TLS), and align the 3DE to the PCI 3DS Core Security Standard baseline.

2. Engagement Details

Engagement type	Grey-box penetration test of the EMV 3-D Secure environment (3DE)
Objective	Identify and safely demonstrate weaknesses in the EMV 3-D Secure Server and its integration endpoints that affect authentication-result integrity and sensitive-data handling; support PCI 3DS, PCI DSS and DORA assurance.
Standards & frameworks	EMVCo EMV 3-D Secure Protocol & Core Functions Specification; PCI 3DS Core Security Standard v1.0 [VERIFY: confirm current version]; NIST SP 800-115; CVSS v4.0
Compliance drivers	PCI 3DS Core Security Standard v1.0 [VERIFY]; PCI DSS v4.0 (3DE in CDE); DORA — Reg. (EU) 2022/2554 (Art. 24–25)
Environment	Dedicated staging instance of the 3DE mirroring production configuration
Approach	Authenticated grey-box testing of the 3DSS message flows and browser integration, with protocol-level message manipulation
Testing window	1 June 2026 – 5 June 2026 (5 business days)
Retest	15 June 2026 (24 hours after remediation) — all findings re-tested and confirmed closed
Report date	7 June 2026 (initial) · 16 June 2026 (final, incl. retest)
Assessment team	Lead Consultant (OSCP, OSWE, CREST CRT); Consultant (OSCP, eWPTX); Technical Reviewer / QA (CREST CCT App, OSCP)

3. Scope

3.1 In-Scope Assets

Asset	Address / Boundary	Description
3DS Server (3DSS)	3ds.paynova.example	EMV 3-D Secure Server
3DS message intake	3ds.paynova.example/3ds/*	AReq/ARes, CReq/CRes endpoints
3DS Method (browser)	3ds.paynova.example	3DS Method iframe / device data collection
Merchant integration API	3ds.paynova.example/result	Authentication-result API

3.2 Out of Scope

- The 3DS SDK (mobile) and ACS/Directory-Server systems operated by other parties.
- Application-layer testing of the wider platform (Web Application & API report, GS-PT-2026-0481).
- Network-layer and segmentation testing (Network report, GS-PT-2026-0482).
- Denial-of-service and physical testing.

3.3 Assumptions, Exclusions & Limitations

- Testing was time-boxed; absence of a finding does not guarantee absence of all vulnerabilities.
- Testing was performed against staging; configuration drift from production is a residual risk to be managed by the Client.
- Destructive actions and bulk data extraction were avoided in line with the Rules of Engagement; exploitation was limited to safe proof-of-concept.
- Findings reflect the state of the assessed systems during the testing window only.

4. Rules of Engagement

- Written authorization was obtained from the Client prior to testing; testing was confined to in-scope assets.
- Testing was conducted against staging during agreed hours, with an emergency contact available throughout.
- No denial-of-service techniques were used; data extraction was limited to the minimum needed to evidence a finding.
- Any critical finding posing immediate risk was reported to the Client without delay (D-01 were flagged in real time).
- All test data and evidence are handled per the data-handling terms (Appendix G) and securely destroyed after the retention period.

5. Methodology

5.1 Approach

A grey-box methodology was used against a staging 3DE. Testing combined manual protocol analysis of the EMV 3-D Secure message flows (AReq/ARes, CReq/CRes, 3DS Method) with web/API testing of the integration endpoints, focusing on authentication-result integrity and sensitive-data handling. Standards: EMVCo EMV 3-D Secure Specification and the PCI 3DS Core Security Standard.

5.2 Standards & Frameworks

- EMVCo EMV 3-D Secure Protocol & Core Functions Specification — protocol behaviour and message integrity
- PCI 3DS Core Security Standard v1.0 [VERIFY: confirm current version vs draft v2.0] — 3DE security baseline (Part 1) and 3DS-specific requirements (Part 2)
- NIST SP 800-115 and OWASP WSTG v4.2 — technical testing process for the integration endpoints
- CVSS v4.0 — vulnerability severity scoring

5.3 Testing Phases

Phase	Coverage
3DE mapping	3DSS endpoints, message flows and integration boundary
Authentication integrity	ARes/CRes signature, transStatus, replay/nonce binding
Sensitive-data handling	CAVV / authentication-value exposure in responses and logs
Client integration	3DS Method iframe, postMessage, device data collection
Cryptography & transport	TLS configuration of the 3DS endpoints
Configuration & errors	Security headers, error handling, input validation

5.4 Tooling

Burp Suite Professional, a bespoke 3-D Secure message-manipulation harness, testssl.sh, nuclei and supporting scripts. All activity was throttled and scoped per the Rules of Engagement.
Evidence handling. Findings are evidenced with redacted transcripts and annotated captures (e.g. Figure 3). Full, unredacted evidence — including screenshots — is retained in the secure project record and made available to the Client and, where applicable, the QSA.

5.5 Risk Rating Methodology

Each finding is scored with CVSS v4.0 (base) and assigned a final business risk rating using a likelihood × impact matrix that accounts for data sensitivity and exploitability in context. Severity bands:

Rating	CVSS v4.0	Definition
Critical	9.0 – 10.0	Immediate, business-critical exposure; remediate within days.
High	7.0 – 8.9	Serious weakness; remediate within weeks.
Medium	4.0 – 6.9	Address in the normal remediation cycle.
Low	0.1 – 3.9	Best-practice hardening.
Informational	N/A	Observation with no direct security risk.

Likelihood Ratings

Likelihood	Definition
High	Readily exploitable by a typical attacker with low effort and no special conditions.
Medium	Exploitable with moderate effort, specific preconditions, or some level of privilege.
Low	Difficult to exploit; requires significant effort, chained conditions, or a privileged position.

Risk Matrix (Likelihood × Impact)

Likelihood ↓ / Impact →	Low	Medium	High	Critical
High	Medium	High	Critical	Critical
Medium	Low	Medium	High	Critical
Low	Low	Low	Medium	High

CVSS scope. *Scores are CVSS v4.0 Base metrics; Threat and Environmental metrics were not applied. The final risk rating combines the CVSS base band with the likelihood × impact assessment and the sensitivity of the affected data.*

6. Findings Summary

ID	Finding	Severity	CVSS	Status
D-01	3DS Server Accepts Forged / Unsigned ARes — Authentication-Result Integrity Bypass	**Critical**	9.4	**Closed**
D-02	CAVV / Authentication Value Exposed in API Responses and Logs	**High**	7.1	**Closed**
D-03	3DS Method Iframe postMessage Origin Not Validated	**Medium**	6.2	**Closed**
D-04	ARes / CRes Replay — Missing Transaction-ID / Nonce Binding	**High**	8.3	**Closed**
D-05	Weak TLS on 3DS Endpoints	**Medium**	6.3	**Closed**
D-06	Missing Security Headers and Verbose Errors on the 3DS Server	**Medium**	6.9	**Closed**

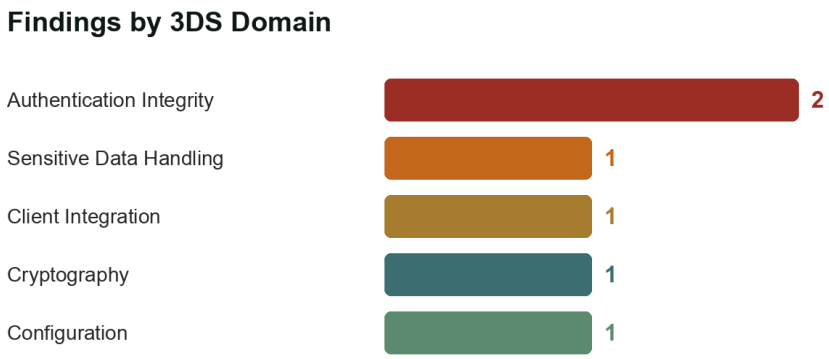

Figure 2 — Findings by 3DS domain.

7. Framework Mapping

This mapping shows evidentiary support toward each framework's testing provisions; it is not a certification or attestation.

Findings and methodology map to the testing provisions of the frameworks below using a three-tier status: Directly addresses (a pentest is the named requirement), Provides evidence supporting (a pentest is accepted evidence, not the mandate), and Conforms to (methodology). Items out of this report's scope are marked Separate engagement.

Framework / Requirement	Status	Basis
PCI 3DS Core Security Standard v1.0 — Part 1 (baseline) + Part 2 (3DS-specific); periodic 3DE penetration test	**Directly addresses**	Penetration test of the 3DE against the 3DS Core baseline and 3DS-specific requirements. [VERIFY: confirm current standard version (v1.0 vs draft v2.0) and the exact penetration-testing requirement number and cadence against the current PCI SSC document.]
PCI DSS v4.0 (the 3DE is typically within CDE scope; Req 11.4)	**Provides evidence supporting**	Where the 3DE falls within PCI DSS scope, this test provides supporting penetration-testing evidence; full Req 11.4 coverage requires the application (GS-PT-2026-0481) and network (GS-PT-2026-0482) reports.
DORA — Art. 24–25 (testing of ICT tools & systems)	**Directly addresses**	Penetration test of an ICT payment-authentication system feeding the ICT risk-management framework. TLPT (Art. 26–27) is a separate engagement.
ISO/IEC 27001:2022 — A.8.8, A.8.29	**Provides evidence supporting**	Technical-vulnerability management and security testing in development and acceptance.
NIS2 — Dir. (EU) 2022/2555 Art. 21(2)(e)–(f)	**Supports**	Security in acquisition/development and policies to assess the effectiveness of risk-management measures.
NIST SP 800-115	**Conforms to (methodology)**	The engagement methodology conforms to this recognized testing standard.

7.1 Scope Boundaries & Separate Assessments

- PCI 3DS vs PCI DSS: the PCI 3DS Core Security Standard governs the 3DE specifically; where the 3DE is also in PCI DSS scope, PCI DSS Req 11.4 is satisfied by the Web Application & API (GS-PT-2026-0481) and Network (GS-PT-2026-0482) reports together — not by this 3DS report alone.
- DORA Art. 26–27 (Threat-Led Penetration Testing / TLPT) is a separate, threat-led engagement type and is not represented by this assessment.
- PCI PIN Security is not a penetration test; it is a key-management / HSM / dual-control assessment (PCI PIN Security Requirements + ASC X9 TR-39), handled by Grilli Security as a separate assessment service.

8. Detailed Findings

D-01 — 3DS Server Accepts Forged / Unsigned ARes — Authentication-Result Integrity Bypass

Severity	**CRITICAL**	**CVSS v4.0**	**9.4**
3DS Domain	EMV 3DS — Authentication Integrity	**3DS / EMVCo Ref**	EMVCo 3DS Spec / PCI 3DS Core
CWE	CWE-345, CWE-347	**Standard**	—
Component	3ds.paynova.example (3DS Server)	**Status**	**Closed — Verified**
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:H/SI:H/SA:N		

Description
The 3DS Server accepted an Authentication Response (ARes) whose cryptographic authenticity was not validated, allowing a forged ARes indicating successful authentication (transStatus=Y) to be accepted. The integrity of the 3-D Secure authentication result was not enforced.

Business Impact
An attacker able to inject or modify the ARes can cause unauthenticated transactions to be treated as successfully authenticated, defeating the core purpose of 3-D Secure (fraud prevention / liability shift) and enabling fraudulent authorization.

Likelihood
Medium-High — requires a position to inject/modify the ARes (a manipulated Directory Server response or MITM), but the absence of signature validation removes the only barrier.

Affected Endpoints
- POST https://3ds.paynova.example/3ds/ares (3DSS message intake)

Steps to Reproduce
1. Capture a 3-D Secure authentication flow and its ARes message.
2. Craft an ARes with transStatus=Y and an invalid/absent signature.
3. Submit it to the 3DSS and confirm it is accepted as a successful authentication.

Evidence (redacted)
```
ARes {transStatus:'Y', signature:'<invalid>'}  ->  3DSS accepts; CRes issued as authenticated  [REDACTED]
```

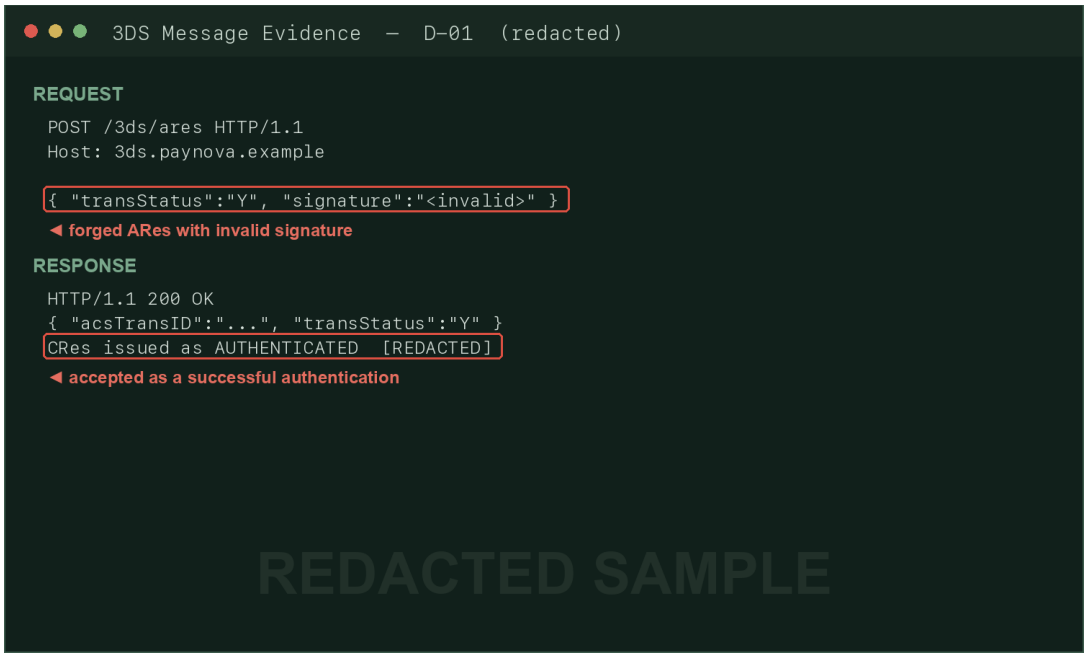

Figure 3 — Annotated 3-D Secure message evidence for D-01 (redacted).

Remediation

1. Validate the cryptographic signature/authenticity of every ARes against the trusted Directory Server keys; reject unsigned or invalid messages.
2. Pin the expected message structure and reject malformed/forged fields.
3. Log and alert on signature-validation failures.

References & Mappings

EMVCo EMV 3-D Secure Protocol & Core Functions Specification · PCI 3DS Core Security Standard v1.0 [VERIFY: requirement number] · CWE-345, CWE-347 · PCI DSS v4.0 (3DE in CDE)

Retest Result

Closed — Remediation Verified (15 June 2026). ARes signature validation enforced; forged/unsigned messages are rejected.

D-02 — CAVV / Authentication Value Exposed in API Responses and Logs

Severity	**HIGH**	**CVSS v4.0**	**7.1**
3DS Domain	EMV 3DS — Sensitive Data Handling	**3DS / EMVCo Ref**	PCI 3DS Core / EMVCo 3DS
CWE	CWE-532, CWE-200	**Standard**	—
Component	3ds.paynova.example	**Status**	**Closed — Verified**
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N		

Description

The Cardholder Authentication Verification Value (CAVV) and related authentication values were returned in API responses to the merchant integration and written to application logs in cleartext.

Business Impact

Exposure of authentication values can facilitate replay/fraud and is a sensitive-data-handling failure within the 3DE; such values must be protected and must not be logged.

Likelihood
Medium — requires authenticated integration or log access, but the data is highly sensitive.

Affected Endpoints
- GET https://3ds.paynova.example/3ds/result/{id}
- Application log: /var/log/3ds/auth.log

Steps to Reproduce
1. Complete a 3-D Secure flow and inspect the result API response for CAVV.
2. Review accessible logs for CAVV / authentication values.

Evidence (redacted)

```
{"cavv":"AAABB...[REDACTED]","eci":"05"}  returned to the merchant and written to logs
```

Remediation
1. Do not expose CAVV/authentication values beyond what the protocol strictly requires, and never log them.
2. Mask/scrub sensitive 3DS values in logs and restrict log access.
3. Review retention and access controls for 3DE logs.

References & Mappings
EMVCo EMV 3-D Secure Specification · PCI 3DS Core Security Standard v1.0 [VERIFY: requirement number] · CWE-532, CWE-200

Retest Result
Closed — Remediation Verified (15 June 2026). CAVV removed from responses and scrubbed from logs.

D-03 — 3DS Method Iframe postMessage Origin Not Validated

Severity	MEDIUM	**CVSS v4.0**	**6.2**
3DS Domain	EMV 3DS — Client Integration	**3DS / EMVCo Ref**	EMVCo 3DS Method
CWE	CWE-346	**Standard**	—
Component	3ds.paynova.example (3DS Method iframe)	**Status**	**Closed — Verified**
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:L/VA:N/SC:H/SI:L/SA:N		

Description
The 3DS Method browser flow processed postMessage events without validating the message origin and reflected threeDSMethodData into the page, enabling cross-origin message injection.

Business Impact
An attacker page could inject or manipulate 3DS Method data, potentially influencing device-data collection or injecting content into the integration context.

Likelihood
Medium — requires luring the cardholder's browser to attacker-controlled content during the flow.

Affected Endpoints
- 3DS Method iframe on 3ds.paynova.example

Steps to Reproduce
1. Host a page that posts a crafted message to the 3DS Method iframe.
2. Observe the message accepted without origin validation.

Evidence (redacted)

```
window.postMessage({threeDSMethodData:'<injected>'}, '*')  ->  accepted; no origin check
```

Remediation
1. Validate the origin of all postMessage events against an allow-list.
2. Encode/validate threeDSMethodData; set a strict CSP frame-ancestors policy.
3. Treat all cross-origin messages as untrusted.

References & Mappings
EMVCo EMV 3-D Secure Specification (3DS Method) · OWASP WSTG-CLNT-11 · CWE-346

Retest Result
Closed — Remediation Verified (15 June 2026). postMessage origin validation and CSP implemented.

D-04 — ARes / CRes Replay — Missing Transaction-ID / Nonce Binding

Severity	**HIGH**	**CVSS v4.0**	**8.3**
3DS Domain	EMV 3DS — Authentication Integrity	**3DS / EMVCo Ref**	EMVCo 3DS Spec / PCI 3DS Core
CWE	CWE-294	**Standard**	—
Component	3ds.paynova.example	**Status**	**Closed — Verified**
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:H/VA:N/SC:L/SI:L/SA:N		

Description
Authentication messages were not bound to a unique, single-use transaction identifier/nonce, allowing a previously-valid ARes/CRes to be replayed to authenticate a different transaction.

Business Impact
Replay of a valid authentication result can authorize fraudulent transactions, defeating the integrity guarantees of the 3-D Secure flow.

Likelihood
Medium — requires capture of a valid message and a replay window.

Affected Endpoints
- POST https://3ds.paynova.example/3ds/cres

Steps to Reproduce
1. Capture a valid ARes/CRes for transaction A.
2. Replay it within the flow for transaction B.
3. Confirm the replayed authentication is accepted.

Evidence (redacted)

```
Replay CRes(txnA) into txnB  ->  accepted as authenticated  [REDACTED]
```

Remediation
1. Bind every authentication message to a unique threeDSServerTransID/nonce and reject reuse.
2. Enforce single-use and short validity windows; track consumed identifiers.
3. Validate transaction-context consistency end-to-end.

References & Mappings
EMVCo EMV 3-D Secure Specification · PCI 3DS Core Security Standard v1.0 [VERIFY: requirement number] · CWE-294

Retest Result
Closed — Remediation Verified (15 June 2026). Per-transaction nonce binding enforced; replays are rejected.

D-05 — Weak TLS on 3DS Endpoints

Severity	MEDIUM	**CVSS v4.0**	**6.3**
3DS Domain	EMV 3DS — Cryptography	**3DS / EMVCo Ref**	PCI 3DS Core / NIST SP 800-115
CWE	CWE-326	**Standard**	—
Component	TLS on 3ds.paynova.example	**Status**	**Closed — Verified**
CVSS Vector	CVSS:4.0/AV:N/AC:H/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N		

Description
The 3DS endpoints offered TLS 1.0/1.1 and weak cipher suites.

Business Impact
A cryptographic-strength gap on a payment-authentication boundary, with downgrade exposure.

Likelihood
Low-Medium.

Affected Endpoints
- TLS on 3ds.paynova.example

Steps to Reproduce
1. Scan the 3DS endpoints' TLS configuration.
2. Confirm legacy protocols/ciphers are offered.

Evidence (redacted)

```
testssl 3ds.paynova.example  ->  TLS 1.0/1.1 enabled; weak ciphers
```

Remediation
1. Disable TLS 1.0/1.1; require TLS 1.2+ and restrict to strong ciphers; enable HSTS.

References & Mappings
PCI 3DS Core Security Standard v1.0 [VERIFY: requirement number] · NIST SP 800-115 · CWE-326 · PCI DSS v4.0 Req 4.2.1

Retest Result
Closed — Remediation Verified (15 June 2026). Legacy TLS disabled; strong configuration enforced.

D-06 — Missing Security Headers and Verbose Errors on the 3DS Server

Severity	MEDIUM	**CVSS v4.0**	**6.9**
3DS Domain	EMV 3DS — Configuration	**3DS / EMVCo Ref**	PCI 3DS Core / OWASP
CWE	CWE-693, CWE-209	**Standard**	—
Component	3ds.paynova.example	**Status**	**Closed — Verified**
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N		

Description
3DS Server responses omitted key security headers (CSP, HSTS, X-Content-Type-Options) and returned verbose error messages disclosing internal details.

Business Impact

Reduced defence-in-depth and information disclosure that aids targeting of a payment-authentication component.

Likelihood
Medium.

Affected Endpoints
- HTTP responses on 3ds.paynova.example

Steps to Reproduce
1. Inspect response headers and error responses.
2. Confirm missing headers and verbose errors.

Evidence (redacted)

```
HTTP/1.1 500  stack trace returned; no CSP / HSTS / X-Content-Type-Options
```

Remediation
1. Deploy CSP, HSTS, X-Content-Type-Options and a strict referrer policy.
2. Return generic errors and log details server-side only.

References & Mappings
PCI 3DS Core Security Standard v1.0 [VERIFY: requirement number] · OWASP WSTG-CONF-07 / ERRH-01 · CWE-693, CWE-209 · PCI DSS v4.0 Req 6.4.1

Retest Result
Closed — Remediation Verified (15 June 2026). Security headers deployed and generic error handling implemented.

9. Remediation & Retest

All findings were remediated by the Client within one week of report delivery and independently re-tested on 15 June 2026 (24 hours after remediation). Section 9.1 sets out the prioritized remediation plan and tracking; Section 9.2 records the retest outcome. Per-finding detail appears in Section 8.

9.1 Prioritized Remediation Plan

ID	Finding	Priority	Effort	Owner	Done
D-01	3DS Server Accepts Forged / Unsigned ARes — Authentication-Result Integrity Bypass	**P1**	M	3DS Engineering	09 Jun 2026
D-02	CAVV / Authentication Value Exposed in API Responses and Logs	**P2**	S	3DS Engineering	11 Jun 2026
D-03	3DS Method Iframe postMessage Origin Not Validated	**P2**	S	Frontend / 3DS	11 Jun 2026
D-04	ARes / CRes Replay — Missing Transaction-ID / Nonce Binding	**P2**	M	3DS Engineering	12 Jun 2026
D-05	Weak TLS on 3DS Endpoints	**P3**	S	DevOps / Edge	13 Jun 2026
D-06	Missing Security Headers and Verbose Errors on the 3DS Server	**P3**	S	3DS Engineering	13 Jun 2026

Priority: P1 immediate (≤7 days) · P2 high (≤2 weeks) · P3 planned (≤1 month) · P4 backlog. **Effort:** S < 1 day · M 1–3 days · L > 3 days. All items completed and verified at retest.

9.2 Retest Results

Every finding was confirmed closed at retest. Per-finding retest detail appears in Section 8.

ID	Finding	Severity	Retest Result
D-01	3DS Server Accepts Forged / Unsigned ARes — Authentication-Result Integrity Bypass	**Critical**	**PASS — Closed**
D-02	CAVV / Authentication Value Exposed in API Responses and Logs	**High**	**PASS — Closed**
D-03	3DS Method Iframe postMessage Origin Not Validated	**Medium**	**PASS — Closed**
D-04	ARes / CRes Replay — Missing Transaction-ID / Nonce Binding	**High**	**PASS — Closed**
D-05	Weak TLS on 3DS Endpoints	**Medium**	**PASS — Closed**
D-06	Missing Security Headers and Verbose Errors on the 3DS Server	**Medium**	**PASS — Closed**

Outcome. Critical findings were remediated within 2 days of report delivery; full remediation across all 6 findings completed within one week, and retesting was performed 24 hours after remediation. Retest passed on first review and the supporting evidence was suitable for PCI assessor (QSA) acceptance.

10. Conclusion

The assessment found a critical authentication-result integrity bypass in the 3DS Server (forged/unsigned ARes accepted), with a replay weakness, sensitive-value exposure and integration issues. The Client remediated all 6 findings, independently verified as closed within the retest window.
Subject to maintaining the remediations and aligning the 3DE to the PCI 3DS Core Security Standard, the 3DE's residual risk is assessed as LOW. Where the 3DE is also in PCI DSS scope, full Req 11.4 coverage is provided by the application (GS-PT-2026-0481) and network (GS-PT-2026-0482) reports together.

10.1 Next Steps & Contact

- Maintain ARes/CRes signature validation and per-transaction nonce binding in production.
- Operationalize the prioritized plan (Section 9.1) and align the 3DE to the PCI 3DS Core Security Standard baseline.
- Re-test the 3DE periodically per the PCI 3DS requirement [VERIFY: cadence] and after significant change.
- Contact Grilli Security at lime@grillisecurity.com for the next assessment.

Appendix A — Severity & CVSS Methodology

Severity bands and CVSS v4.0 ranges are defined in Section 5.5. CVSS base scores were calculated using the FIRST.org CVSS v4.0 calculator; full vector strings are recorded per finding in Section 8. Final business risk ratings incorporate data sensitivity and contextual exploitability.

Appendix B — 3DS / PCI 3DS Coverage Checklist

The table below records coverage of the 3DE testing areas (EMVCo 3DS / PCI 3DS Core) against the in-scope 3DSS and integration. Tested = exercised, no issue or covered by hardening; → D-xx = yielded the referenced finding; N/A = not applicable / out of scope.

3DS Test Area	Description	Result
3DS-01	3DS Server message intake (AReq/ARes)	Tested
3DS-02	ARes signature / authenticity validation	→ **D-01**
3DS-03	ARes / CRes replay & nonce binding	→ **D-04**
3DS-04	transStatus / authentication-result integrity	→ **D-01**
3DS-05	CAVV / authentication-value handling	→ **D-02**
3DS-06	3DS Method (iframe) data collection	→ **D-03**
3DS-07	postMessage / cross-origin messaging	→ **D-03**
3DS-08	Challenge flow (CReq/CRes) handling	Tested
3DS-09	Directory Server integration trust	Tested
3DS-10	ACS interaction / redirect handling	Tested
3DS-11	Sensitive data in transit (TLS)	→ **D-05**
3DS-12	Sensitive data at rest / logging	→ **D-02**
3DS-13	Security headers / error handling	→ **D-06**
3DS-14	Authentication & session of 3DS APIs	Tested
3DS-15	Input validation / injection on 3DS endpoints	Tested
3DS-16	3DS SDK (mobile) integration	**N/A**

Appendix C — Tooling

Burp Suite Professional, a bespoke 3-D Secure message-manipulation harness, testssl.sh, nuclei and supporting scripts. All activity was throttled and scoped per the Rules of Engagement.

Appendix D — PCI DSS v4.0 & DORA Cross-Reference

The PCI 3DS Core Security Standard governs the 3DE and is directly supported by this report [VERIFY: requirement number/cadence]. Where the 3DE is also within PCI DSS scope, PCI DSS Req 11.4 is satisfied by the Web Application & API (GS-PT-2026-0481) and Network (GS-PT-2026-0482) reports together. DORA Art. 24–25 are supported as part of the ICT risk-management framework; DORA Art. 26–27 TLPT is a separate engagement.

Appendix E — Glossary

- **BOLA/IDOR —** Broken Object-/Function-Level Authorization / Insecure Direct Object Reference

- **CDE —** Cardholder Data Environment (PCI DSS)
- **3DE —** 3-D Secure Environment
- **CVSS —** Common Vulnerability Scoring System (v4.0)
- **DORA —** Digital Operational Resilience Act (EU 2022/2554)
- **EMVCo —** EMV company governing the EMV 3-D Secure specification
- **MFA —** Multi-Factor Authentication
- **NIS2 —** Directive (EU) 2022/2555 on network & information security
- **QSA —** Qualified Security Assessor (PCI)
- **TLPT —** Threat-Led Penetration Testing (DORA Art. 26–27)
- **3DSS —** 3-D Secure Server
- **ACS —** Access Control Server (issuer side)
- **ARes/CRes —** Authentication Response / Challenge Response messages
- **CAVV —** Cardholder Authentication Verification Value

Appendix F — Assessment Team & Qualifications

The engagement was delivered by certified offensive-security consultants (certifications include OSCP, OSWE, eWPTX, CREST CRT and CREST CCT Application). Individual identities are recorded in the secure project record and anonymized in this sample. Quality assurance was performed by an independent senior reviewer prior to issue.

Appendix G — Data Handling, Confidentiality & Disclaimer

All evidence and test artefacts are stored encrypted, access-controlled, and destroyed after the agreed retention period. This report is provided for the Client's internal security and compliance use and does not by itself constitute a compliance certification. It reflects the state of the assessed systems during the testing window and does not guarantee the absence of all vulnerabilities. Remediation should be validated in a controlled environment. Grilli Security accepts no liability for actions taken on the basis of this report.