

Continuous Security Testing Report

AIBIDIA OY
AIBIDIA

Table of Contents

Assessment of the Target’s Security 3

Executive summary 4

Findings and actions in latest test cycle 6

Conducted test cycles 8

Summary of findings 9

Unremediated findings 9

Remediated findings 10

Findings 11

Appendix 1: Target system analysis 54

Assessment of the Target's Security

OVERALL  Exposed	Critical findings —
TARGET Aibidia Oy Aibidia	High risk findings —
	Medium risk findings —
	Low risk findings 4
	Minimal risk findings 8

Grades



Excellent

No findings or only minimal risk findings.



Good

Individual low risk findings.



Exposed

Individual medium risk or several low risk findings.



Vulnerable

Individual high risk or several medium risk findings.



Critical

Individual critical risk or several high risk findings.

Finding risk categories

Critical findings

These findings can often be easily exploited by an unauthenticated or low-privilege remote attacker and may lead to complete system compromise or gaining access to critical information without requiring user interaction.

High risk findings

These findings can easily compromise the confidentiality, integrity or availability of resources. They may allow users to gain more privileges or allow unauthenticated remote users to view resources that should otherwise be protected by access control mechanisms.

Medium risk findings

These findings may be difficult to exploit but could still under certain circumstances lead to some compromise of the confidentiality, integrity or availability of resources. They could have had a Critical impact or High impact but are less easily exploited based on a technical evaluation of the finding.

Low risk findings

This rating is given to all other findings that have a security impact. These are the types of findings that are believed to require unlikely circumstances to be able to be exploited, or where a successful exploit would have minimal consequences.

Minimal risk findings

This rating is given to findings that currently have no security impact. They are typically deviations from security best practises. These findings do not typically affect the overall grade.

Executive summary

Project overview

Silverskin Information Security Oy conducted a security assessment of Aibidia's Aibidia web application and all its included solutions during November and December 2024. The application is used by Aibidia's business customers to manage their transfer pricing as well as perform analysis on the related information. The users log in to the service with a personal username and password or via a Microsoft or Google account. The security assessment has been ordered by Aibidia Oy to ensure the security posture of the application.

Continuous security testing

The goal of continuous security testing is to test the system regularly to discover vulnerabilities that may occur due to changes in the application. Changes can be caused by development of new features, updates to the core components, and through regressions. Vulnerabilities may also be discovered when new attack techniques are invented. Continuous testing helps maintain the security of the system by minimizing the risk of undiscovered vulnerabilities and improves the monitoring of quality and security posture.

This report describes the application's security posture based on the tests performed by 19.03.2026. Continuous security testing will continue under the current agreement.

Assessment scope

The scope of the assessment included the following areas:

- The Aibidia web application and its HTTP APIs, including all functionalities within the end user and admin UIs.
- Vulnerability scanning of the server environment.

Detailed information regarding the conducted tests and testing coverage can be found in Appendix 1: Target System Analysis.

In March 2026, *Financial Transactions (FT)* was removed from the testing scope; this solution has been discontinued. In addition, a new solution, called *Strategic Transfer Pricing Management (STPM)*, was added to the scope.

Methodology

The security assessment was conducted by independent, experienced, and certified auditors of Silverskin Information Security Oy. In the assessment, we utilized offensive security testing techniques to discover any known vulnerabilities and simulated a malicious actor with the goal of gaining unauthorized access to data and functionality of the assessment target. The assessment was conducted utilizing a gray-box approach, meaning that access to the target environment and testing credentials were provided prior to the assessment.

Assessment summary

The latest testing cycle focused on the new solution *Strategic Transfer Pricing Management (STPM)* where features, access controls and impact on the other solutions were tested. A low risk finding was detected, regarding intentional resources consumption.

ITPAurora and DS were also re-tested and a new low risk finding has been reported under the second solution, related to an abuse of the SQL queries functionality.

In addition, several open findings have been checked to verify the remediation implemented. During this verification, a new low risk finding has been discovered during the benchmark creation process, regarding to an intentional resource consumption in the files upload.

Furthermore, an automated vulnerability scan was performed against the server environments.

Conclusions and recommendations

In our professional opinion, and based on assessments conducted so far, the application's security level in its current state is good. The application can withstand common attacks against web applications.

We recommend that the low risk finding *UAC-022 Abuse of Functionality (DS queries)* should be reviewed to determine if a quick remediation must be implemented. The others low risk findings can be remediated as a part of the application's regular update cycle. The minimal risk findings should be reviewed to determine if action is needed to prevent any abuse of the found issues.

Silverskin Information Security Oy
Helsinki 19.03.2026

Findings and actions in latest test cycle

General

- Security level has changed from *Good* to *Exposed*
- System analysis and testing has continued
 - New solution *Strategic Transfer Pricing Management (STPM)*
 - TPAurora
 - DS
- Re-tested findings:
 - UAC-002 Prompt Injection (Minimal)
 - UAC-008 Session Termination (Minimal)
 - UAC-011 Cross-Site Scripting (XSS), Stored (Low)
 - UAC-015 Unrestricted File Upload (DS) (Low)
 - UAC-017 Unrestricted File Upload (FT) (Minimal)
 - UAC-018 Outdated, Obsolete, Or Vulnerable 3rd Party Software Libraries or Frameworks (Pydantic) (Minimal)
- Target system analysis has been updated
 - UAC-008 finding has been moved to General branch in the TSA because it also applies to TPAurora service

Attention needed

- No concerns that would require attention

New findings

- UAC-020 Intentional Resource Consumption (Tax Group) (Low)
- UAC-021 Intentional Resource Consumption (Benchmarks) (Low)
- UAC-022 Abuse of Functionality (DS queries) (Low)

Updates

- *Financial Transactions (FT)* solution, as agreed, has been removed from the testing scope because the product is being discontinued. A reference to this product remains in the Target System Analysis
- UAC-008 Session Termination (Minimal): This finding also applies to TPAurora environment. The details have been updated to include this use case

Remediated findings

- UAC-015 Unrestricted File Upload (DS) (Low)
- UAC-002 Prompt Injection (Minimal)
- UAC-017 Unrestricted File Upload (FT) (Minimal): No remediated, but the product where it belongs (FT) is being discontinued and it is not in scope any longer
- UAC-018 Outdated, Obsolete, Or Vulnerable 3rd Party Software Libraries or Frameworks (Pydantic) (Minimal)

Conducted test cycles

- January 2026: 3 days of specialist work plus reporting (Antonio Lopez)
- December 2025: 3 days of specialist work plus reporting (Antonio Lopez)
- September 2025: 3 days of specialist work plus reporting (Toni Judin)
- June 2025: 3 days of specialist work plus reporting (Toni Judin)
- March 2025: 3 days of specialist work plus reporting (Toni Judin)
- December 2024: Initial security assessment project (Markus Komppa, Ahti Pellinen)

Summary of findings

Unremediated findings

ID	VULNERABILITY	RISK	LEGACY ID	FIRST REPORTED
● UAC-011	Cross-Site Scripting (XSS), Stored	Low	305891	04.12.2024
● UAC-020	Intentional Resource Consumption (Tax Group)	Low	-	17.03.2026
● UAC-021	Intentional Resource Consumption (Benchmarks)	Low	-	18.03.2026
● UAC-022	Abuse of Functionality (DS queries)	Low	-	19.03.2026
● UAC-003	Weak TLS Configuration	Minimal	305892	04.12.2024
● UAC-004	Service Fingerprinting	Minimal	305873	04.12.2024
● UAC-005	Sensitive Information In URLs	Minimal	305875	04.12.2024
● UAC-008	Session Termination	Minimal	312494	13.03.2025
● UAC-009	Path Traversal	Minimal	305870	04.12.2024
● UAC-014	Vulnerable And Outdated Components (DOMPurify)	Minimal	-	17.06.2025
● UAC-016	Improper Error Handling	Minimal	-	16.09.2025
● UAC-019	Liberal Cross-Origin Resource Sharing (dashboards API)	Minimal	-	18.12.2025

Remediated findings

ID	VULNERABILITY	PRIOR RISK	LEGACY ID	FIRST REPORTED	REMEDIED
UAC-006	Sensitive Information In URLs	Low	305874	04.12.2024	18.06.2025
UAC-007	Open Redirection	Low	305889	04.12.2024	12.03.2025
UAC-012	Server-Side Request Forgery	Low	305872	04.12.2024	12.03.2025
UAC-015	Unrestricted File Upload (DS)	Low	-	18.06.2025	17.03.2026
UAC-001	HTML Injection	Minimal	305882	04.12.2024	12.03.2025
UAC-002	Prompt Injection	Minimal	312482	11.03.2025	16.03.2026
UAC-013	Dependency Confusion	Minimal	305883	04.12.2024	17.06.2025
UAC-010	Outdated, Obsolete, Or Vulnerable 3rd Party Software Libraries or Frameworks	Minimal	305890	04.12.2024	12.03.2025
UAC-018	Outdated, Obsolete, Or Vulnerable 3rd Party Software Libraries or Frameworks (Pydantic)	Minimal	-	18.12.2025	19.03.2026

Findings

• UAC-011 Cross-Site Scripting (XSS), Stored

CLASSIFICATION

Low risk programming error

STATUS

Finding reported on 04.12.2024

DESCRIPTION

Cross-Site Scripting (XSS) refers to the inclusion of malicious JavaScript code into a site so that when the page is opened, the victim's browser executes the included code.

Stored XSS allows an attacker to store malicious code in the service database, potentially threatening all users of the service as the code executes every time the page is visited.

IMPACT

Potential impacts for cross-site scripting include, but are not limited to: performing functionalities on behalf of the victim, such as changing their account details, stealing sensitive data, and hijacking sessions / user accounts.

In case of a real attack, it is unlikely for the victim to even notice that anything malicious happened.

REMEDIATION

Validate and sanitize the input on the server side using a centralized allow list based approach. Use output encoding to safely display the data on the page.

REFERENCES

https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html
https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

DETAILS

Update 2026.03.18:

The vulnerability seems to still be present in the application and the current Proof of Concept is valid.

Update 2025.12.16:

The new API domain for the pen-test environment is `platform-api-pen.aibidia.com`. In addition, the example request has been updated.

Original:

The application does not restrict the file upload for benchmark orders and allows the content-type and file extension for the uploaded file to be specified in the request. After creating a benchmark order the email sent to the contact email contains a valid link to the file which allows non authenticated access to the content. The impact of the XSS is extremely limited as the domain that the payload is triggered on is the api domain `app-aibidia-pltf-api-uat.azurewebsites.net`

Steps to reproduce:

- 1) Create a benchmark order request with an attachment with modified file content-type, name and content.
- 2) Open the the attachment from the email sent to the contact address.
- 3) The url after the first redirect opens on the platform api address with XSS.

REQUEST

```
POST /api/BenchmarkOrders HTTP/2
Host: platform-api-pen.aibidia.com
Content-Length: 622
Sec-Ch-Ua-Platform: "macOS"
Authorization: Bearer [REDACTED]
Accept-Language: en-GB,en;q=0.9
Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
Traceparent: 00-5ae156ecdf2443018a7baf926e76e574-c0ab01be5787488a-01
Aibidia-App-Code: pltf
Aibidia-Partner-Databaseid: 7
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/
537.36
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundarygAarcCi0Eo4kGYk4
Accept: */*
Origin: https://platform-pen.aibidia.com
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://platform-pen.aibidia.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

-----WebKitFormBoundarygAarcCi0Eo4kGYk4
Content-Disposition: form-data; name="UseCaseId"

201
-----WebKitFormBoundarygAarcCi0Eo4kGYk4
Content-Disposition: form-data; name="StudyName"
```

```
test
-----WebKitFormBoundarygAarcCi0Eo4kGYk4
Content-Disposition: form-data; name="Comment"

test
-----WebKitFormBoundarygAarcCi0Eo4kGYk4
Content-Disposition: form-data; name="files";
filename="file.html"
Content-Type: text/html

<script>print()</script>
-----WebKitFormBoundarygAarcCi0Eo4kGYk4
Content-Disposition: form-data; name="ContactEmail"

test1@silverskin.fi
-----WebKitFormBoundarygAarcCi0Eo4kGYk4--
```

RESPONSE

```
HTTP/2 201 Created
Date: Tue, 16 Dec 2025 13:45:20 GMT
Access-Control-Allow-Origin: https://platform-pen.aibidia.com
Cache-Control: no-store
Content-Length: 0
X-Ms-Middleware-Request-Id: 000000000-0000-0000-0000-000000000000
Request-Context: appId=cid-v1:a007fa05-cdbd-40f6-a05a-
b76f5c4ba807
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
```

ACCESS LEVEL REQUIRED

N/A

METHOD OF DISCOVERY

Manual

METHOD OF EXPLOITATION

Manual

• UAC-020 Intentional Resource Consumption (Tax Group)

CLASSIFICATION

Low risk design flaw

STATUS

Finding reported on 17.03.2026

DESCRIPTION

It is possible for an attacker to abuse the add tax group functionality in order to use unnecessary amounts of server-side computing resources.

IMPACT

A malicious actor can degrade the performance of the service for other users by consuming large amounts of server-side computing resources, eventually leading to a Denial of Service (DoS) on STPM feature.

REMEDIATION

Enforce, on the server-side, validation for the length of *entityIds* list. In addition, avoid to display too verbose error messages on server responses.

If possible, add a content-length limiter for requests and responses in the service.

REFERENCES

<https://owasp.org/API-Security/editions/2023/en/Oxa4-unrestricted-resource-consumption/>

https://owasp.org/www-community/attacks/Denial_of_Service

DETAILS

There is a lack of server-side validation in the PUT request `"/api/taxgroups/<taxgroup_ID>/entities"`, performed in order to update the map entities under a tax group. If the entity ID doesn't exist, the same error message is repeated for each entity in the response `"Entity <ID> does not exist in the scenario for the forecast period.\n"`. **This makes possible to achieve an amplification of ~1:33 input-output.**

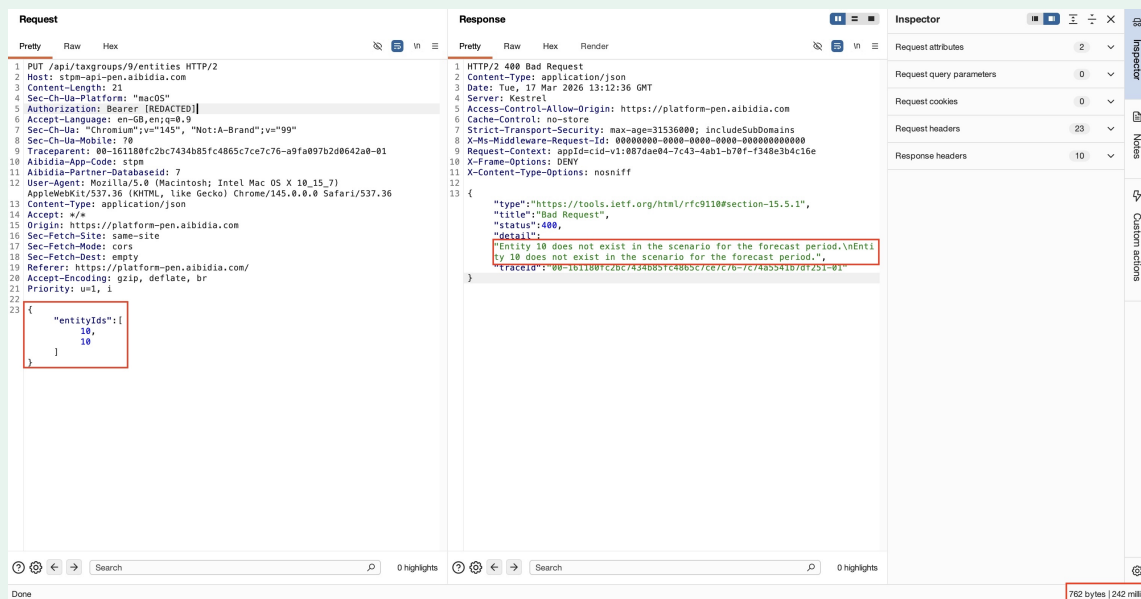
It is important to highlight that some delay, during the attack (sending concurrent requests exploiting this vulnerability, has been caused across tenants for STPM service.

Steps to reproduce:

1. Browse to STPM service
2. Create a year management
3. Create two legal entities under the same tax jurisdiction
4. Create a scenario and select the created legal entities for that scenario (*Selected Legal Entities* tab)
5. Under *Tax Loss*, create a tax group
6. Start to intercept the web traffic with some proxy tool (e.g. Burpsuite)
7. Modify the create tax group, mapping one of the legal entities to the principal entity (*Map Entities to Tax Group* column)
8. A PUT request must have been intercepted to the endpoint `"/api/taxgroups/<taxgroup_ID>/entities"`
9. Modify the *entityIds* list to include multiple non-valid entity IDs (it can be the same ID multiple times, for example 999)
10. Send the modify request to verify the error message is shown for each ID in the list

Screenshot:

The first image shows the reflected error message one time for each same entity ID (notice response length and time).



The second picture demonstrate the issue of repeating the same error message, allowing to craft requests that will trigger long responses, regarding content and time (notice response length and time).

The screenshot shows a web browser's developer tools interface. The 'Request' tab is active, displaying a PUT request to `/api/taxgroups/9/entities` with a status of 200. The 'Response' tab shows a JSON array of entity IDs. The 'Inspector' tab is also visible. The search bar at the bottom indicates 9953 matches.

The third image show the error message displayed to end users via UI when the application takes longer than expected to load.

The screenshot shows a web application loading screen. The header displays the company name 'Aibidia' and the product name 'STPM Strategic Transfer Pricing Management'. A large purple loading spinner is centered on the page. Below the spinner, a message reads: 'WE ARE EXPERIENCING AN UNUSUAL DELAY WHILE LOADING THE APPLICATION. PLEASE WAIT WHILE WE TRY TO RECONNECT...'. The background is a light blue gradient.

REQUEST (UPDATE TAX GROUP ENTITIES)

PUT /api/taxgroups/9/entities HTTP/2
Host: stpm-api-pen.aibidia.com
Content-Length: 21
Sec-Ch-Ua-Platform: "macOS"

```
Authorization: Bearer [REDACTED]
Accept-Language: en-GB,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Traceparent: 00-161180fc2bc7434b85fc4865c7ce7c76-
a9fa097b2d0642a0-01
Aibidia-App-Code: stpm
Aibidia-Partner-Databaseid: 7
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/
537.36
Content-Type: application/json
Accept: */*
Origin: https://platform-pen.aibidia.com
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://platform-pen.aibidia.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{"entityIds":[10,
<--Snipped-->,
10]}
```

RESPONSE (UPDATE TAX GROUP ENTITIES)

```
HTTP/2 400 Bad Request
Content-Type: application/json
Date: Tue, 17 Mar 2026 13:12:36 GMT
Server: Kestrel
Access-Control-Allow-Origin: https://platform-pen.aibidia.com
Cache-Control: no-store
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Ms-Middleware-Request-Id: 00000000-0000-0000-0000-000000000000
Request-Context: appId=cid-v1:087dae04-7c43-4ab1-b70f-
f348e3b4c16e
X-Frame-Options: DENY
X-Content-Type-Options: nosniff

{"type":"https://tools.ietf.org/html/
rfc9110#section-15.5.1","title":"Bad
Request","status":400,"detail":"Entity 10 does not exist in the
scenario for the forecast period.\n,
<--Snipped-->,
Entity 10 does not exist in the scenario for the forecast
period.","traceId":"00-161180fc2bc7434b85fc4865c7ce7c76-7c74a554
1b7df251-01"}
```

ACCESS LEVEL REQUIRED

Administrator

METHOD OF DISCOVERY

Manual

METHOD OF EXPLOITATION

Automated

• UAC-021 Intentional Resource Consumption (Benchmarks)

CLASSIFICATION

Low risk design flaw

STATUS

Finding reported on 18.03.2026

DESCRIPTION

It is possible for an attacker to abuse the benchmark creation process in order to use unnecessary amounts of server-side computing resources.

IMPACT

A malicious actor can degrade the performance of the service for other users by consuming large amounts of server-side computing resources. This issue could eventually lead to a Denial of Service (DoS).

REMEDIATION

Enforce, on the server-side, a restriction to the amount of files that can be uploaded within a single request when creating a benchmark.

REFERENCES

<https://owasp.org/API-Security/editions/2023/en/Oxa4-unrestricted-resource-consumption/>

https://owasp.org/www-community/attacks/Denial_of_Service

DETAILS

There is lack of validation in the file upload functionality during the benchmark creation process regarding to the amount of files that can be uploaded within a single request. It is also possible to upload crafted files which are not valid types, allowing to upload a large amount of files within the total size restriction (10Mb).

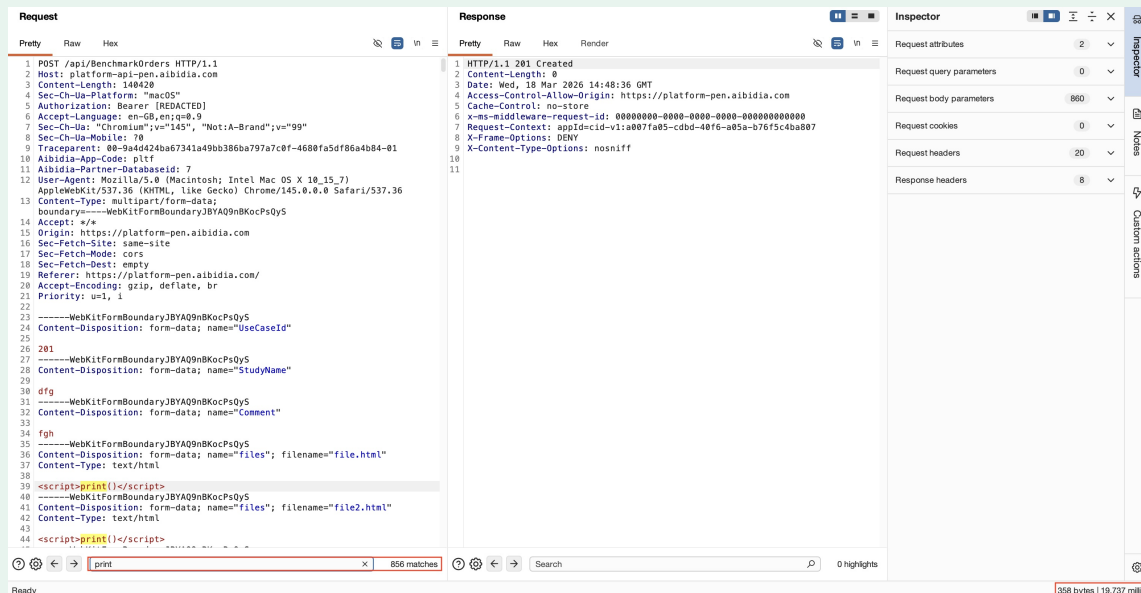
Steps to reproduce:

1. Log in to the service
2. Start the process of creating a bench mark and fill the form
3. Upload a crafted file (e.g. `echo -n "test" > file.pdf`)
4. Start to intercept the web traffic with some proxy tool (e.g. Burpsuite)
5. Click on *Submit*
6. In the intercepted POST request `/api/BenchmarkOrders`, repeat the same file multiple times (see example request)

- Send the tampered request to verify that every time more files are added, the response time increases accordingly, proving the resource consumption

Screenshot:

The next image demonstrates the intentional resource consumption when 856 files were uploaded within a single request.



REQUEST (UPLOAD MULTIPLE FILES CREATING A BENCHMARK)

```
POST /api/BenchmarkOrders HTTP/1.1
Host: platform-api-pen.aibidia.com
Content-Length: 140420
Sec-Ch-Ua-Platform: "macOS"
Authorization: Bearer [REDACTED]
Accept-Language: en-GB,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Traceparent: 00-9a4d424ba67341a49bb386ba797a7c0f-4680fa5df86a4b84-01
Aibidia-App-Code: pltf
Aibidia-Partner-Databaseid: 7
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryJBIAQ9nBKocPsQyS
Accept: */*
Origin: https://platform-pen.aibidia.com
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://platform-pen.aibidia.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

```
-----WebKitFormBoundaryJBYAQ9nBKocPsQyS
Content-Disposition: form-data; name="UseCaseId"

201
-----WebKitFormBoundaryJBYAQ9nBKocPsQyS
Content-Disposition: form-data; name="StudyName"

dfg
-----WebKitFormBoundaryJBYAQ9nBKocPsQyS
Content-Disposition: form-data; name="Comment"

fgh
-----WebKitFormBoundaryJBYAQ9nBKocPsQyS
Content-Disposition: form-data; name="files";
filename="file.html"
Content-Type: text/html

<script>print()</script>
-----WebKitFormBoundaryJBYAQ9nBKocPsQyS
Content-Disposition: form-data; name="files";
filename="file2.html"
Content-Type: text/html

<script>print()</script>
-----WebKitFormBoundaryJBYAQ9nBKocPsQyS
Content-Disposition: form-data; name="files";
filename="file.html"
Content-Type: text/html

<script>print()</script>
-----WebKitFormBoundaryJBYAQ9nBKocPsQyS
Content-Disposition: form-data; name="files";
filename="file2.html"
Content-Type: text/html

<script>print()</script>
<--Snipped large amount of same files-->
-----WebKitFormBoundaryJBYAQ9nBKocPsQyS
Content-Disposition: form-data; name="ContactEmail"

test1@silverskin.fi
-----WebKitFormBoundaryJBYAQ9nBKocPsQyS--
```

RESPONSE (UPLOAD MULTIPLE FILES CREATING A BENCHMARK)

```
HTTP/1.1 201 Created
Content-Length: 0
Date: Wed, 18 Mar 2026 14:48:36 GMT
Access-Control-Allow-Origin: https://platform-pen.aibidia.com
Cache-Control: no-store
x-ms-middleware-request-id: 00000000-0000-0000-0000-000000000000
Request-Context: appId=cid-v1:a007fa05-cdbd-40f6-a05a-b76f5c4ba807
X-Frame-Options: DENY
```

X-Content-Type-Options: nosniff

ACCESS LEVEL REQUIRED
Administrator

METHOD OF DISCOVERY
Manual

METHOD OF EXPLOITATION
Automated

• UAC-022 Abuse of Functionality (DS queries)

CLASSIFICATION

Low risk design flaw

STATUS

Finding reported on 19.03.2026

DESCRIPTION

The *DS* solution offers a feature to run custom SQL queries under *Transforms*. This functionality can be used in an unintended manner, allowing users to map the database structure. Due to time constraints, it is uncertain if inserting data in any other schema than expected could have a higher impact in the service.

This finding has attached two findings which include example scripts and data enumerated:

- example_database_scripts
- database_enumerated_info

IMPACT

A malicious user can create custom queries to map additional information about the database, such a version, user and container IDs, schemas and tables.

REMEDIATION

If possible, filter the error messages to avoid showing the result of queries to users.

REFERENCES

https://owasp.org/www-community/vulnerabilities/Business_logic_vulnerability

https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html

DETAILS

The *DS* solution offers a feature to run custom SQL queries under *Transforms*. The output of the queries is not displayed to the users. The only message shown is under *Transform Run History* if any query returned a error.

Error messages can be quite verbose some times, they can even include the result of a nested query. For example, casting the result of a nested query to integer as below, the error message shows the result of the query:

```
SELECT CAST(@@version AS INT);
```

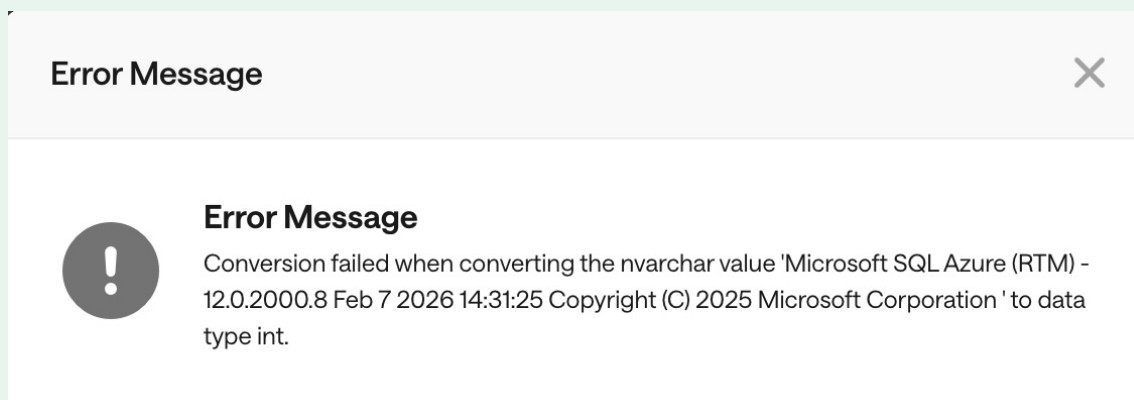
This allows users to abuse the run custom queries feature in order to enumerate the database structure. Due to time constraints, no higher impact was possible to be proven; however, it is highly recommended to void displaying too verbose messages to end users.

Steps to reproduce:

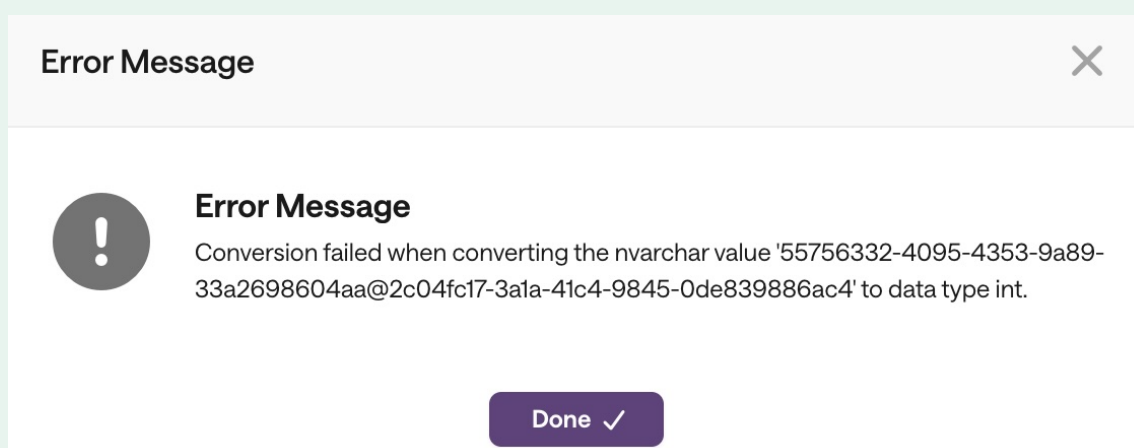
1. Log in to the service and open the *DS* module
2. Create a custom query under *Scripts*. For example, the previous code will return the version of the database
3. Run the query under *Transforms* which should return an error
4. Open the latest query run information under *Transform Run History*
5. Verify the database version is returned in the error

Screenshot:

The first image shows the error message for `SELECT CAST(@@version AS INT);` script.



The second picture shows the error message for `SELECT CAST(SYSTEM_USER AS INT);`



ACCESS LEVEL REQUIRED

Authenticated

METHOD OF DISCOVERY

Manual

METHOD OF EXPLOITATION

Manual

• UAC-003 Weak TLS Configuration

CLASSIFICATION

Minimal risk misconfiguration

STATUS

Finding reported on 04.12.2024

DESCRIPTION

The server supports weak TLS encryption algorithms and protocol versions.

IMPACT

The use of weak encryption algorithms or protocols could potentially allow Manipulator-in-the-Middle (MitM) attacks where an attacker can read and modify data presumed to be encrypted.

REMEDIATION

Disable the listed encryption algorithms.

To achieve post-quantum safety, it is recommended to support only quantum safe TLS 1.3 algorithms like AES256 and CHACHA20.

REFERENCES

https://cheatsheetseries.owasp.org/cheatsheets/TLS_Cipher_String_Cheat_Sheet.html
<https://www.ssh.com/academy/cryptography/what-is-quantum-safe-cryptography>
<https://ciphersuite.info/>
<https://www.ssllabs.com/>

DETAILS

2025.12.15 update:

All the Azure hosts now only support TLS 1.3 cipher and they use post-quantum algorithms.

Weak TLS 1.2 ciphers supported for platform-uat.aibidia.com:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

Weak TLS 1.2 ciphers supported for platform-pen.aibidia.com and dashboards- uat.aibidia.com:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

2025.03.12 finding updated:

Almost all of the hosts for apis and for the application use the same ciphers.

Weak TLS 1.2 ciphers supported:

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

Except app-aibidia-panintelligence-uat.azurewebsites.net supports these weak TLS 1.2 ciphers:

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

ACCESS LEVEL REQUIRED

Network

METHOD OF DISCOVERY

Automated

METHOD OF EXPLOITATION

Manual

• UAC-004 Service Fingerprinting

CLASSIFICATION

Minimal risk misconfiguration

STATUS

Finding reported on 04.12.2024

DESCRIPTION

The system discloses information about the services it uses and their versions.

platform-uat Server Microsoft-IIS/10.0 header

IMPACT

The leakage of detailed information about the service environment, such as the software used and their exact version numbers, can make it easier for attackers to discover and exploit known vulnerabilities.

REMEDIATION

If possible, disable banners and headers that disclose information about the services and versions used.

REFERENCES

https://owasp.org/www-project-automated-threats-to-web-applications/assets/oats/EN/OAT-004_Fingerprinting.html
https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server

DETAILS

Currently, the following services expose their Server in the response headers:

app-aibidia-broker-uat.azurewebsites.net:
Server: Microsoft-IIS/10.0

app-aibidia-dsapi-uat.azurewebsites.net:
Server: Kestrel

app-aibidia-ft-api-uat.azurewebsites.net:
Server: Kestrel

app-aibidia-nltx-svc-uat.azurewebsites.net:
Server: Kestrel

app-aibidia-otpm-api-uat.azurewebsites.net:

Server: Kestrel

url9161.aibidia.com:

Server: nginx

Example of full response headers can be seen in the next section.

REQUEST

```
POST /hub/negotiate?negotiateVersion=1 HTTP/2
Host: app-aibidia-broker-uat.azurewebsites.net
Content-Length: 0
Cache-Control: max-age=0
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer [Removed for readability]
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
Sec-Ch-Ua-Mobile: ?0
X-Signalr-User-Agent: Microsoft SignalR/7.0 (7.0.10; Unknown OS;
Browser; Unknown Runtime Version)
Traceparent: 00-
a2bfa41d548e4afd9cb5210c0e7af421-272f7e3522ca49c9-01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Accept: */*
Origin: https://platform-uat.aibidia.com
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://platform-uat.aibidia.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

RESPONSE

```
HTTP/2 200 OK
Content-Type: application/json
Date: Wed, 20 Nov 2024 14:49:59 GMT
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: https://platform-uat.aibidia.com
Set-Cookie:
ARRAffinity=f00e06a6082d9d1c6e5c2dc56408c7d59586e6b62b7d6ffb75ed
6adf485e0042;Path=/;HttpOnly;Secure;Domain=app-aibidia-broker-
uat.azurewebsites.net
Set-Cookie:
ARRAffinitySameSite=f00e06a6082d9d1c6e5c2dc56408c7d59586e6b62b7d
6ffb75ed6adf485e0042;Path=/;HttpOnly;SameSite=None;Secure;Domain
=app-aibidia-broker-uat.azurewebsites.net
Vary: Origin,Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubDomains
```

X-Ms-Middleware-Request-Id: 00000000-0000-0000-0000-000000000000
Request-Context: appId=cid-v1:34132976-a0af-4f49-88ba-3f17789153de
X-Powered-By: ASP.NET

```
{"negotiateVersion":1,"connectionId":"6y4RycRFIiOabKqL5BwmUQ","connectionToken":"m1qWHHfSGDexuaZw5a-g5Q","availableTransports":[{"transport":"WebSockets","transferFormats":["Text","Binary"]}, {"transport":"ServerSentEvents","transferFormats":["Text"]}, {"transport":"LongPolling","transferFormats":["Text","Binary"]}]}
```

ACCESS LEVEL REQUIRED

N/A

METHOD OF DISCOVERY

Automated

METHOD OF EXPLOITATION

N/A

• UAC-005 Sensitive Information In URLs

CLASSIFICATION

Minimal risk design flaw

STATUS

Finding reported on 04.12.2024

DESCRIPTION

The application passes sensitive information into URL paths or query parameters. Simply using HTTPS does not resolve this vulnerability.

Sensitive information within URLs may be logged in various locations, including the user's browser, the web server, and any forward or reverse proxy servers between the two endpoints.

URLs may also be displayed on-screen, bookmarked, or emailed around by users. They may be disclosed to third parties via the Referer -header when any off-site links are followed. In addition, URL parameters may be saved to 3rd party link scanning or archiving services.

Placing sensitive data such as session tokens into the URL increases the risk that they will be captured by an attacker.

The Aibidia platform uses websockets to communicate between front- and back-end services. When opening the socket connection, the application authenticates with the endpoint by passing users session token (JWT) to the service as a HTTP GET query parameter.

IMPACT

Regardless of the encryption (HTTPS) used, the URL parameters could be exposed in the following locations:

- Referer -header
- Server Logs
- Shared Systems
- Browser History
- Browser Cache
- Shared links

REMEDIATION

Applications should use an alternative mechanism for transmitting sensitive information, such as HTTP cookies or POST request bodies.

Use single use access token to establish websocket connections with URL query parameter instead of users session token.

Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: https://platform-uat.aibidia.com
Upgrade: websocket
Vary: Origin
Strict-Transport-Security: max-age=31536000; includeSubDomains
x-ms-middleware-request-id: 00000000-0000-0000-0000-000000000000
Request-Context: appId=cid-v1:34132976-a0af-4f49-88ba-3f17789153de
Sec-WebSocket-Accept: 51zCpF47iFgfYgyohuaV6nIWHFY=
X-Powered-By: ASP.NET

REQUEST #2

GET /hub?Aibidia-Partner-
Databaseid=7&id=ezhNmhSxdEZNavYX717QZQ&access_token=<access_JWT>
HTTP/2
Host: broker-pen.aibidia.com
Connection: Upgrade
Pragma: no-cache
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/
537.36
Upgrade: websocket
Origin: https://platform-pen.aibidia.com
Sec-WebSocket-Version: 13
Accept-Encoding: gzip, deflate, br
Accept-Language: en-GB,en;q=0.9
Sec-WebSocket-Key: CNCNwXhHx3es8reb6jU4fg==

RESPONSE #2

HTTP/1.1 101 Switching Protocols
Connection: Upgrade
Date: Tue, 16 Dec 2025 09:46:21 GMT
Access-Control-Allow-Origin: https://platform-pen.aibidia.com
Upgrade: websocket
x-ms-middleware-request-id: 00000000-0000-0000-0000-000000000000
Sec-WebSocket-Accept: l2H0WUAdEpY5mApngaDT6csVw4=

ACCESS LEVEL REQUIRED

Authenticated User

METHOD OF DISCOVERY

Automated

METHOD OF EXPLOITATION
N/A

• UAC-008 Session Termination

CLASSIFICATION

Minimal risk programming error

STATUS

Finding reported on 13.03.2025

DESCRIPTION

The application does not end the user's session correctly after logging out and the session token is not properly deleted or invalidated.

IMPACT

It is possible for an attacker to continue using a hijacked session identifier even if the victim has logged out of the service.

REMEDIATION

Implement proper session management controls and make sure to invalidate the session when the user logs out.

If the session identifier/token itself cannot be directly invalidated (e.g., due to a third-party implementation), ensure automatic expiration and check the token against a deny list so that it is no longer accepted by the system once the user has ended the session.

For more detailed instructions regarding JWT tokens, see References.

REFERENCES

https://cheatsheetseries.owasp.org/cheatsheets/JSON_Web_Token_for_Java_Cheat_Sheet.html#no-built-in-token-revocation-by-the-user
https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

DETAILS

Update 2026.03.16:

Since TPAurora is in a different environment, a new request has been added to example the issue in that service.

Update 2025.12.16:

The example request (see request #1) has been updated to demonstrate this issue remains in the new pen-test environment.

Original:

The logout functionality does not terminate usage of access tokens and there seems to be no way for users to terminate their tokens in a situation when for example a malware steals user's browser storage. The access token has 1 hour expiration timer and refresh token has 1 day expiration timer which is reasonable.

Steps to reproduce:

- 1) Login to the application with any user
- 2) Take note of the user's session token
- 3) Logout from the application
- 4) Send any request that requires authentication to the application using the logged out user's token

REQUEST #1 (PLATFORM)

```
GET /api/Account/user HTTP/2
Host: platform-api-pen.aibidia.com
Authorization: Bearer [Logged out user's test1@silverskin.fi
access token]
```

RESPONSE #1 (PLATFORM)

```
HTTP/2 200 OK
Content-Type: application/json; charset=utf-8
Date: Tue, 16 Dec 2025 09:26:39 GMT
Access-Control-Allow-Origin: https://platform-pen.aibidia.com
Cache-Control: no-store
X-Ms-Middleware-Request-Id: 000000000-0000-0000-0000-000000000000
Request-Context: appId=cid-v1:a007fa05-cdbd-40f6-a05a-
b76f5c4ba807
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
```

```
{"Id":9,"UserId":5,"UserObjectId":"635eca0b-000d-45cf-99f1-
c08a8f6dbe93","Upn":"test1@silverskin.fi","FullName":"Silverskin
1","AppCodes":
["tpdoc"],"DatabaseId":7,"DatabaseName":"pentenant009529","Serve
rName":"sql-aibidia-
pen.database.windows.net","IssuerTenantId":"5929a6f5-912b-4c2d-8
dde-06a66f89a286"}
```

REQUEST #2 (TPAURORA)

```
GET /user/profile HTTP/1.1
Host: tpaurora-uat.azurewebsites.net
Cookie: [REDACTED]
Sec-Ch-Ua-Platform: "macOS"
Accept-Language: en-GB,en;q=0.9
Sec-Ch-Ua: "Chromium";v="145", "Not:A-Brand";v="99"
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
```

```
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://tpaurora-uat.azurewebsites.net/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
Connection: keep-alive
```

RESPONSE #2 (TPAURORA)

```
HTTP/1.1 200 OK
Content-Length: 508
Content-Type: application/json
Date: Mon, 16 Mar 2026 16:03:52 GMT
Server: uvicorn
Strict-Transport-Security: max-age=31536000; includeSubDomains
x-ms-middleware-request-id: e662a5c4-f8bb-4a83-98c1-eaff456b9299
```

```
{"email":"test3@silverskin.fi","firstName":"test3","fullName":"test3 silverskin","hasSubscription":false,"id":"1a8aa42c-defa-4a59-a9cc-d3a02c53b6a5","initials":"TS","lastName":"silverskin","monthlyPromptCount":1,"monthlyPromptLimit":-1,"onboardingVideoShown":true,"role":"user","subscriptionEndDate":"","subscriptionStartDate":"","subscriptionType":"trial","trialDaysLeft":25,"trialDaysTotal":30,"trialEndDate":"2026-04-09T17:28:15.716378","trialExpired":false,"trialStartDate":"2026-03-10T17:28:15.716378"}
```

ACCESS LEVEL REQUIRED

N/A

METHOD OF DISCOVERY

Manual

METHOD OF EXPLOITATION

N/A

• UAC-009 Path Traversal

CLASSIFICATION

Minimal risk programming error

STATUS

Finding reported on 04.12.2024

DESCRIPTION

A path traversal attack (also known as directory traversal) aims to access files and directories that are stored outside the web root folder.

By manipulating parameters that reference files with “dot-dot-slash (../)” sequences and its variations or by using absolute file paths, it may be possible to access files and directories stored in the file system.

It should be noted that access to files is limited by system operational access control.

TPDoc Document Preview API allows users to traverse a single directory down. Possibly due to the microservice architecture and other constraints, the exploitability is assessed to be limited, as the user does not have access to the operating system files.

IMPACT

A malicious user can gain access to unintended server-side local files that the application has access to. In this case, the reach is limited and no sensitive file system files are available, but the existence of this issue indicates lack of relevant input controls.

REMEDIATION

Avoid working with user input when using file system calls.

Ensure the user cannot supply all parts of the path – surround it with your path code. Validate user input.

REFERENCES

https://owasp.org/www-community/attacks/Path_Traversal

DETAILS

Steps to reproduce:

- 1) Login to the application
- 2) Navigate to TPDoc and generate Document Preview local file
- 3) Capture the request the application fetches the document from /api/documents/previews?fileName=[filename]
- 4) Modify the requests fileName-parameter to include path traversal payload "../previews/" + the original filename
- 5) Release the request and verify, that the intended file is returned in the response

REQUEST

```
GET /api/documents/previews?fileName=../previews/asdadasd%20-%20Local%20File%20Preview%20-%202029.c3240ff1-4d2a-449a-acde-aaefd4aff846.pdf HTTP/2
Host: app-aibidia-tpdoc-api-uat.azurewebsites.net
Sec-Ch-Ua-Platform: "Linux"
Authorization: Bearer [REMOVED FOR READABILITY]
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
Sec-Ch-Ua-Mobile: ?0
Traceparent: 00-5ef8f6c962f240368aff4ee2a68c0cc8-a583aee0e7a14efb-01
Aibidia-App-Code: tpdoc
Aibidia-Partner-Databaseid: 848
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
Content-Type: application/json
Selectedyearid: 202
Accept: */*
Origin: https://platform-uat.aibidia.com
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://platform-uat.aibidia.com/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

RESPONSE

```
HTTP/2 200 OK
Content-Type: application/pdf
Date: Mon, 18 Nov 2024 16:57:36 GMT
Access-Control-Allow-Origin: https://platform-uat.aibidia.com
Access-Control-Expose-Headers: Content-Disposition
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Ms-Middleware-Request-Id: 00000000-0000-0000-0000-000000000000
Request-Context: appId=cid-v1:399a361b-41aa-4b3a-86f4-2aed06cedf3a

%PDF-1.5
```

4 0 obj
[SNIPPED FOR READABILITY]

ACCESS LEVEL REQUIRED
Authenticated User

METHOD OF DISCOVERY
Manual

METHOD OF EXPLOITATION
Automated

• UAC-014 Vulnerable And Outdated Components (DOMPurify)

CLASSIFICATION

Minimal risk misconfiguration

STATUS

Finding reported on 17.06.2025

DESCRIPTION

The software versions are not up to date. Outdated components can contain known vulnerabilities.

IMPACT

An attacker may use known vulnerabilities, for example, to gain access or extract sensitive information from the server.

REMEDIATION

Regularly check and update outdated / vulnerable 3rd party components.

REFERENCES

https://cheatsheetseries.owasp.org/cheatsheets/Vulnerable_Dependency_Management_Cheat_Sheet.html
<https://github.com/advisories/GHSA-vhxf-7vqr-mrjg>

DETAILS

Outdated and vulnerable components:

- DOMPurify (Multiple versions)

REQUEST #1 (DOMPURIFY 2.5.7)

GET /tpdoc/assets/index-B_PPhmic.js HTTP/2
Host: platform-uat.aibidia.com

RESPONSE #1 (DOMPURIFY 2.5.7)

HTTP/2 200 OK
Content-Type: application/javascript;charset=utf-8
Date: Tue, 17 Jun 2025 13:38:50 GMT
Accept-Ranges: bytes
Cache-Control: private
Content-Md5: JWc5kwTi1thN/ym1rUQFxA==

Etag: "0x8DDAA6A87CB9C04"
Last-Modified: Fri, 13 Jun 2025 11:07:47 GMT
Content-Length: 3773155
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Ms-Request-Id: c200a90d-801e-0015-3d8d-df70eb000000
X-Ms-Version: 2018-03-28
Referrer-Policy: strict-origin-when-cross-origin
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'self'; script-src 'self'
https://cdn.aibidia.com/pyramid/ 'sha256-3oCEUY6pDcTx0j/
If07xFg9j//NLBbRX1KtksKnUAdo='; style-src 'self' 'unsafe-inline'
https://cdn.aibidia.com/pyramid/ https://api.mapbox.com/styles/
v1/ https://fonts.googleapis.com/ https://cdn.vitally.io; font-
src 'self' https://fonts.gstatic.com/s/barlow/ data;; img-src
'self' data: blob;; child-src blob;; frame-src 'self' https://
dashboards-uat.aibidia.com https://login.microsoftonline.com/;
connect-src https://app-aibidia-nltx-svc-uat.azurewebsites.net
https://dashboards-uat.aibidia.com https://js.monitor.azure.com/
scripts/b/ai.config.1.cfg.json https://
aibidiab2cuat.b2clogin.com/ https://app-aibidia-
baseclassifiersapi-uat.azurewebsites.net/api/ https://func-
aibidia-excelgen-uat.azurewebsites.net/api/ExcelExport https://
app-aibidia-broker-uat.azurewebsites.net/hub/ wss://app-aibidia-
broker-uat.azurewebsites.net/hub https://app-aibidia-tmapi-
uat.azurewebsites.net/api/ https://app-aibidia-tpdoc-api-
uat.azurewebsites.net/api/ https://app-aibidia-pltf-api-
uat.azurewebsites.net/api/ https://app-aibidia-wfmapi-
uat.azurewebsites.net/api/ https://app-aibidia-cplapi-
uat.azurewebsites.net/api/ https://app-analytics-serviceapi-
uat.azurewebsites.net/api/ https://app-aibidia-pyramidproxy-
uat.azurewebsites.net https://api.mapbox.com https://
*.tiles.mapbox.com https://events.mapbox.com/events/v2 https://
westeurope-5.in.applicationinsights.azure.com/v2/track https://
dc.services.visualstudio.com/v2/track https://
login.microsoftonline.com https://api.vitally-eu.io/ https://
app.vitally-eu.io/; object-src 'none'

[Redacted]

```
/*! @license DOMPurify 2.5.7 | (c) Cure53 and other contributors  
| Released under the Apache license 2.0 and Mozilla Public  
License 2.0 | github.com/cure53/DOMPurify/blob/2.5.7/LICENSE */
```

[Redacted]

REQUEST #2 (DOMPURIFY 3.1.7)

GET /ds/assets/TransformEditor-BSunFHZK.js HTTP/2
Host: platform-uat.aibidia.com

RESPONSE #2 (DOMPURIFY 3.1.7)

HTTP/2 200 OK

Content-Type: application/javascript;charset=utf-8

Date: Tue, 17 Jun 2025 13:45:06 GMT

Accept-Ranges: bytes

Cache-Control: private

Content-Md5: 6hXuTT35xhJGSh6BAwun6g==

Etag: "0x8DD9F7D9E84A0D0"

Last-Modified: Fri, 30 May 2025 13:26:43 GMT

Content-Length: 3971883

Strict-Transport-Security: max-age=31536000; includeSubDomains

X-Ms-Request-Id: 9fc4813b-201e-0026-638e-df0ec7000000

X-Ms-Version: 2018-03-28

Referrer-Policy: strict-origin-when-cross-origin

X-Content-Type-Options: nosniff

X-Frame-Options: SAMEORIGIN

Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-eval' 'sha256-

xZ4Mf8yt6TP9YX84i6ucshY7p+24jainxqDggTEs0GE=' https://
cdn.aibidia.com/pyramid/; style-src 'self' 'unsafe-inline'
https://cdn.aibidia.com/pyramid/ https://api.mapbox.com/styles/
v1/ https://fonts.googleapis.com/; font-src 'self' https://
fonts.gstatic.com/s/barlow/; worker-src https://app-aibidia-
dsapi-uat.azurewebsites.net//monacoeditorwork/
editor.worker.bundle.js blob:; img-src 'self' data: blob:;
child-src blob:; frame-src 'self' https://
aibidiab2cuat.b2clogin.com; connect-src 'self' https://
js.monitor.azure.com/scripts/b/ai.config.1.cfg.json https://app-
aibidia-dsapi-uat.azurewebsites.net/ https://
westeurope-5.in.applicationinsights.azure.com/v2/track https://
aibidiab2cuat.b2clogin.com https://app-aibidia-pltf-api-
uat.azurewebsites.net/ https://func-aibidia-excelgen-
uat.azurewebsites.net/api/ https://app-aibidia-broker-
uat.azurewebsites.net wss://app-aibidia-broker-
uat.azurewebsites.net https://app-analytics-serviceapi-
uat.azurewebsites.net/api/ https://app-aibidia-pyramidproxy-
uat.azurewebsites.net/infraEntryPoint https://api.mapbox.com
https://*.tiles.mapbox.com https://events.mapbox.com/events/v2;
object-src 'none'

[Redacted]

/*! @license DOMPurify 3.1.7 | (c) Cure53 and other contributors
| Released under the Apache license 2.0 and Mozilla Public
License 2.0 | github.com/cure53/DOMPurify/blob/3.1.7/LICENSE *

[Redacted]

ACCESS LEVEL REQUIRED

N/A

METHOD OF DISCOVERY

Automated

METHOD OF EXPLOITATION

Manual

• UAC-016 Improper Error Handling

CLASSIFICATION

Minimal risk misconfiguration

STATUS

Finding reported on 16.09.2025

DESCRIPTION

In the event of an error, the application returns an error message to the user which discloses information about how the application functions.

IMPACT

An attacker can find sensitive information about the application's operations and operating environment through error messages. Sensitive information may help to plan and implement further attacks.

REMEDIATION

Implement generalized error handling that always returns generic error messages to users. More detailed errors should only be logged on the server-side.

REFERENCES

https://cheatsheetseries.owasp.org/cheatsheets/Error_Handling_Cheat_Sheet.html

DETAILS

When request body is removed from the CSV export request, Java stacktrace is returned in response.

REQUEST

```
POST /pi/export/csv HTTP/1.1
Host: dashboards-uat.aibidia.com
Cookie:
BENDERISGREAT=HP7vylnuj2Vre8hYYuKBZDPVu3CXo8ucBCz5CvEeAEK507c8xu
;
_hp2_id.2896365371=%7B%22userId%22%3A%22765112910924803%22%2C%22
pageviewId%22%3A%227271737643743060%22%2C%22sessionId%22%3A%2225
66547267278352%22%2C%22identity%22%3Anull%2C%22trackerVersion%22
%3A%224.0%22%7D
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15;
rv:142.0) Gecko/20100101 Firefox/142.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
```

Content-Length: 0
Origin: https://dashboards-uat.aibidia.com
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Priority: u=0
Te: trailers
Connection: keep-alive

RESPONSE

HTTP/1.1 200 OK
Content-Type: application/json;charset=UTF-8
Date: Tue, 16 Sep 2025 14:13:35 GMT
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: https://dashboards-uat.aibidia.com
Vary: Origin
Content-Security-Policy: frame-ancestors https://platform-
uat.aibidia.com; form-action 'self';
Referrer-Policy: no-referrer
Feature-Policy: geolocation 'none'; midi 'none'; notifications
'none'; push 'none'; sync-xhr 'none'; microphone 'none'; camera
'none'; magnetometer 'none'; gyroscope 'none'; speaker 'none';
vibrate 'none'; fullscreen 'none'; payment 'none';
Permissions-Policy:
geolocation=(),midi=(),notifications=(),push=(),syncxhr=(),micro
phone=(),camera=(),magnetometer=(),gyroscope=(),speaker=(),vibra
te=(),fullscreen=(),payment=()
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Pi-Has-Data: false
Pi-Error-Message: One or more recipients does not have
permission to view the contents of an attachment
Pi-Supports-Data-Presence-Flag: true
Content-Disposition: attachment; filename=null.csv
Content-Length: 10057

```
{"errorMessage":null,"messageCode":null,"requestUrl":null,"reque  
stMethod":"POST","statusCode":403,"appVersion":"pi.2025_08","sql  
":"","stacktrace":"com.panintelligence.chart.FetchChartException  
\n\tat java.base/  
jdk.internal.reflect.NativeConstructorAccessorImpl.newInstance0(  
Native Method)\n\tat java.base/  
jdk.internal.reflect.NativeConstructorAccessorImpl.newInstance(U  
nknown Source)\n\tat java.base/  
jdk.internal.reflect.DelegatingConstructorAccessorImpl.newInstan  
ce(Unknown Source)\n\tat java.base/  
java.lang.reflect.Constructor.newInstanceWithCaller(Unknown  
Source)\n\tat java.base/  
java.lang.reflect.Constructor.newInstance(Unknown Source)\n\tat  
org.codehaus.groovy.reflection.CachedConstructor.invoke(CachedCo  
nstructor.java:72)\n\tat
```

```
org.codehaus.groovy.runtime.callsite.ConstructorSite$Constructor
SiteNoUnwrapNoCoerce.callConstructor(ConstructorSite.java:105)\n
\tat
org.codehaus.groovy.runtime.callsite.CallSiteArray.defaultCallCo
nstructor(CallSiteArray.java:59)\n\tat
org.codehaus.groovy.runtime.callsite.AbstractCallSite.callConstr
uctor(AbstractCallSite.java:263)\n\tat
org.codehaus.groovy.runtime.callsite.AbstractCallSite.callConstr
uctor(AbstractCallSite.java:268)\n\tat
com.panintelligence.chart.FetchChartException.create(FetchChartE
xception.groovy:37)\n\tat java.base/
jdk.internal.reflect.NativeMethodAccessorImpl.invoke0(Native
Method)\n\tat java.base/
jdk.internal.reflect.NativeMethodAccessorImpl.invoke(Unknown
Source)\n\tat java.base/
jdk.internal.reflect.DelegatingMethodAccessorImpl.invoke(Unknown
Source)\n\tat java.base/java.lang.reflect.Method.invoke(Unknown
Source)\n\tat
org.codehaus.groovy.reflection.CachedMethod.invoke(CachedMethod.
java:107)\n\tat
org.codehaus.groovy.runtime.callsite.StaticMetaMethodSite$Static
MetaMethodSiteNoUnwrapNoCoerce.invoke(StaticMetaMethodSite.java:
149)\n\tat
org.codehaus.groovy.runtime.callsite.StaticMetaMethodSite.callSt
atic(StaticMetaMethodSite.java:100)\n\tat
org.codehaus.groovy.runtime.callsite.CallSiteArray.defaultCallSt
atic(CallSiteArray.java:55)\n\tat
org.codehaus.groovy.runtime.callsite.AbstractCallSite.callStatic
(AbstractCallSite.java:217)\n\tat
org.codehaus.groovy.runtime.callsite.AbstractCallSite.callStatic
(AbstractCallSite.java:231)\n\tat
com.panintelligence.chart.FetchChartException.createWhenUserHasN
oAccessToChart(FetchChartException.groovy:46)\n\tat
com.panintelligence.GrailsChartDomainDrivenService.createFetchCh
artRequestAndResponse(GrailsChartDomainDrivenService.groovy:187)
\n\tat
com.panintelligence.GrailsChartDomainDrivenService$createFetchCh
artRequestAndResponse$2.callCurrent(Unknown Source)\n\tat
org.codehaus.groovy.runtime.callsite.CallSiteArray.defaultCallCu
rrent(CallSiteArray.java:51)\n\tat
com.panintelligence.GrailsChartDomainDrivenService$createFetchCh
artRequestAndResponse$2.callCurrent(Unknown Source)\n\tat
com.panintelligence.GrailsChartDomainDrivenService.fetchChartReq
uestResponsePackage(GrailsChartDomainDrivenService.groovy:137)\n
\tat
com.panintelligence.GrailsChartDomainDrivenService.fetchChartReq
uestResponsePackageForChart(GrailsChartDomainDrivenService.groov
y:112)\n\tat
com.panintelligence.GrailsChartDomainDrivenService$fetchChartReq
uestResponsePackageForChart$0.call(Unknown Source)\n\tat
org.codehaus.groovy.runtime.callsite.CallSiteArray.defaultCall(C
allSiteArray.java:47)\n\tat
com.panintelligence.GrailsChartDomainDrivenService$fetchChartReq
uestResponsePackageForChart$0.call(Unknown Source)\n\tat
com.panintelligence.GrailsDownloadService.createDataOnlyResponse
```

```
(GrailsDownloadService.groovy:40)\n\tat  
com.panintelligence.GrailsDownloadService$createDataOnlyResponse  
.call(Unknown Source)\n\tat  
com.panintelligence.ExportController.csv(ExportController.groovy  
:231)\n\tat  
org.grails.core.DefaultGrailsControllerClass$MethodHandleInvoker  
.invoke(DefaultGrailsControllerClass.java:223)\n\tat  
org.grails.core.DefaultGrailsControllerClass.invoke(DefaultGrail  
sControllerClass.java:188)\n\tat  
org.grails.web.mapping.mvc.UrlMappingsInfoHandlerAdapter.handle(  
UrlMappingsInfoHandlerAdapter.groovy:90)\n\tat  
org.springframework.web.servlet.DispatcherServlet.doDispatch(Dis  
patcherServlet.java:1072)\n\tat  
org.springframework.web.servlet.DispatcherServlet.doService(Disp  
atcherServlet.java:965)\n\tat  
org.springframework.web.servlet.FrameworkServlet.processRequest(  
FrameworkServlet.java:1006)\n\tat  
org.springframework.web.servlet.FrameworkServlet.doPost(Framewor  
kServlet.java:909)\n\tat  
javax.servlet.http.HttpServlet.service(HttpServlet.java:555)\n\tat  
org.springframework.web.servlet.FrameworkServlet.service(Framewo  
rkServlet.java:883)\n\tat  
javax.servlet.http.HttpServlet.service(HttpServlet.java:623)\n\tat  
org.apache.catalina.core.ApplicationFilterChain.internalDoFilter  
(ApplicationFilterChain.java:199)\n\tat  
org.apache.catalina.core.ApplicationFilterChain.doFilter(Applica  
tionFilterChain.java:144)\n\tat  
org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.ja  
va:51)\n\tat  
org.apache.catalina.core.ApplicationFilterChain.internalDoFilter  
(ApplicationFilterChain.java:168)\n\tat  
org.apache.catalina.core.ApplicationFilterChain.doFilter(Applica  
tionFilterChain.java:144)\n\tat  
org.apache.catalina.filters.HttpHeaderSecurityFilter.doFilter(Ht  
tpHeaderSecurityFilter.java:129)\n\tat  
org.apache.catalina.core.ApplicationFilterChain.internalDoFilter  
(ApplicationFilterChain.java:168)\n\tat  
org.apache.catalina.core.ApplicationFilterChain.doFilter(Applica  
tionFilterChain.java:144)\n\tat  
javax.servlet.FilterChain$doFilter.call(Unknown Source)\n\tat  
com.panintelligence.security.filters.PiSecurityFilter.doFilter(P  
iSecurityFilter.groovy:82)\n\tat  
org.apache.catalina.core.ApplicationFilterChain.internalDoFilter  
(ApplicationFilterChain.java:168)\n\tat  
org.apache.catalina.core.ApplicationFilterChain.doFilter(Applica  
tionFilterChain.java:144)\n\tat  
org.grails.web.servlet.mvc.GrailsWebRequestFilter.doFilterIntern  
al(GrailsWebRequestFilter.java:77)\n\tat  
org.springframework.web.filter.OncePerRequestFilter.doFilter(On  
cePerRequestFilter.java:117)\n\tat  
org.apache.catalina.core.ApplicationFilterChain.internalDoFilter  
(ApplicationFilterChain.java:168)\n\tat  
org.apache.catalina.core.ApplicationFilterChain.doFilter(Applica
```

```
tionFilterChain.java:144)\n\tat  
org.grails.web.filters.HiddenHttpMethodFilter.doFilterInternal(H  
iddenHttpMethodFilter.java:67)\n\tat  
org.springframework.web.filter.OncePerRequestFilter.doFilter(Once  
PerRequestFilter.java:117)\n\tat  
org.apache.catalina.core.ApplicationFilterChain.internalDoFilter  
(ApplicationFilterChain.java:168)\n\tat  
org.apache.catalina.core.ApplicationFilterChain.doFilter(Applica  
tionFilterChain.java:144)\n\tat  
org.springframework.web.filter.CharacterEncodingFilter.doFilterI  
nternal(CharacterEncodingFilter.java:201)\n\tat  
org.springframework.web.filter.OncePerRequestFilter.doFilter(Once  
PerRequestFilter.java:117)\n\tat  
org.apache.catalina.core.ApplicationFilterChain.internalDoFilter  
(ApplicationFilterChain.java:168)\n\tat  
org.apache.catalina.core.ApplicationFilterChain.doFilter(Applica  
tionFilterChain.java:144)\n\tat  
org.springframework.boot.actuate.metrics.web.servlet.WebMvcMetri  
csFilter.doFilterInternal(WebMvcMetricsFilter.java:96)\n\tat  
org.springframework.web.filter.OncePerRequestFilter.doFilter(Once  
PerRequestFilter.java:117)\n\tat  
org.apache.catalina.core.ApplicationFilterChain.internalDoFilter  
(ApplicationFilterChain.java:168)\n\tat  
org.apache.catalina.core.ApplicationFilterChain.doFilter(Applica  
tionFilterChain.java:144)\n\tat  
org.springframework.boot.web.servlet.support.ErrorPageFilter.doF  
ilter(ErrorPageFilter.java:126)\n\tat  
org.springframework.boot.web.servlet.support.ErrorPageFilter.acc  
ess$000(ErrorPageFilter.java:64)\n\tat  
org.springframework.boot.web.servlet.support.ErrorPageFilter$1.d  
oFilterInternal(ErrorPageFilter.java:101)\n\tat  
org.springframework.web.filter.OncePerRequestFilter.doFilter(Once  
PerRequestFilter.java:117)\n\tat  
org.springframework.boot.web.servlet.support.ErrorPageFilter.doF  
ilter(ErrorPageFilter.java:119)\n\tat  
org.apache.catalina.core.ApplicationFilterChain.internalDoFilter  
(ApplicationFilterChain.java:168)\n\tat  
org.apache.catalina.core.ApplicationFilterChain.doFilter(Applica  
tionFilterChain.java:144)\n\tat  
org.springframework.web.filter.CorsFilter.doFilterInternal(CorsF  
ilter.java:91)\n\tat  
org.springframework.web.filter.OncePerRequestFilter.doFilter(Once  
PerRequestFilter.java:117)\n\tat  
org.apache.catalina.core.ApplicationFilterChain.internalDoFilter  
(ApplicationFilterChain.java:168)\n\tat  
org.apache.catalina.core.ApplicationFilterChain.doFilter(Applica  
tionFilterChain.java:144)\n\tat  
org.apache.catalina.core.StandardWrapperValve.invoke(StandardWra  
pperValve.java:168)\n\tat  
org.apache.catalina.core.StandardContextValve.invoke(StandardCon  
textValve.java:90)\n\tat  
org.apache.catalina.authenticator.AuthenticatorBase.invoke(Authe  
nticatorBase.java:482)\n\tat  
org.apache.catalina.core.StandardHostValve.invoke(StandardHostVa  
lve.java:130)\n\tat
```

```
org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:93)\n\tat\norg.apache.catalina.valves.AbstractAccessLogValve.invoke(AbstractAccessLogValve.java:656)\n\tat\norg.apache.catalina.core.StandardEngineValve.invoke(StandardEngineValve.java:74)\n\tat\norg.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:346)\n\tat\norg.apache.coyote.http11.Http11Processor.service(Http11Processor.java:397)\n\tat\norg.apache.coyote.AbstractProcessorLight.process(AbstractProcessorLight.java:63)\n\tat\norg.apache.coyote.AbstractProtocol$ConnectionHandler.process(AbstractProtocol.java:935)\n\tat\norg.apache.tomcat.util.net.NioEndpoint$SocketProcessor.doRun(NioEndpoint.java:1826)\n\tat\norg.apache.tomcat.util.net.SocketProcessorBase.run(SocketProcessorBase.java:52)\n\tat\norg.apache.tomcat.util.threads.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1189)\n\tat\norg.apache.tomcat.util.threads.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:658)\n\tat\norg.apache.tomcat.util.threads.TaskThread$WrappingRunnable.run(TaskThread.java:63)\n\tat\n\tat java.base/java.lang.Thread.run(Unknown Source)\n", "errors": [], "invalidRecords":\n[], "invalidRecordColumns":\n[], "errorPanelTableHeaderForDescription": null}}
```

ACCESS LEVEL REQUIRED

Authenticated user

METHOD OF DISCOVERY

Manual

METHOD OF EXPLOITATION

Manual

• UAC-019 Liberal Cross-Origin Resource Sharing (dashboards API)

CLASSIFICATION

Minimal risk misconfiguration

STATUS

Finding reported on 18.12.2025

DESCRIPTION

Cross-Origin Resource Sharing (CORS) can enable cross-site HTTP requests and allow access to selected resources for requests from a different origin than where the requested resource is located.

For example, a web client could make an AJAX request to a resource on some other domain.

IMPACT

Resource sharing is allowed with any origin. In some cases, this could potentially lead to information leakage or Cross-Site-Request-Forgery (CSRF).

REMEDIATION

Configure the Access-Control-Allow-Origin response header to only allow a specific origin.

If multiple origins are required, validate the value of the Origin request header against a list of allowed origins on the server side and echo that origin in the Access-Control-Allow-Origin header.

REFERENCES

https://cheatsheetseries.owasp.org/cheatsheets/HTML5_Security_Cheat_Sheet.html#cross-origin-resource-sharing
<https://developer.mozilla.org/en-US/docs/Web/HTTP/CORS>

DETAILS

The API `dashboards-pen.aibidia.com` allows access to its resources for requests made from any origin.

It is important to highlight that this is an informational finding, but it can still be chain with future findings in order to achieve a higher impact.

REQUEST

POST /pi/chart/show HTTP/2
Host: dashboards-pen.aibidia.com
Cookie: [REDACTED]
Content-Length: 2189
Sec-Ch-Ua-Platform: "macOS"
Accept-Language: en-GB,en;q=0.9
Sec-Ch-Ua: "Chromium";v="143", "Not A(Brand";v="24"
Sec-Ch-Ua-Mobile: ?0
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36
Accept: */*
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: *
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

categoryId=94&categoryObjectCriteria=<!--Snippet-->

RESPONSE

HTTP/2 200 OK
Date: Thu, 18 Dec 2025 09:55:31 GMT
Access-Control-Allow-Credentials: true
Access-Control-Allow-Origin: *
Cache-Control: no-cache, no-store
Pragma: no-cache
Set-Cookie: BENDERISGREAT=; SameSite=None; HttpOnly; Path=/pi;
Partitioned; Secure; Max-Age=0;
Vary: Origin
Content-Length: 0
Content-Security-Policy: frame-ancestors https://platform-pen.aibidia.com; form-action 'self';
Referrer-Policy: no-referrer
Feature-Policy: geolocation 'none'; midi 'none'; notifications 'none'; push 'none'; sync-xhr 'none'; microphone 'none'; camera 'none'; magnetometer 'none'; gyroscope 'none'; speaker 'none'; vibrate 'none'; fullscreen 'none'; payment 'none';
Permissions-Policy: geolocation=(),midi=(),notifications=(),push=(),syncxhr=(),microphone=(),camera=(),magnetometer=(),gyroscope=(),speaker=(),vibrate=(),fullscreen=(),payment=()
X-Frame-Options: DENY
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff

ACCESS LEVEL REQUIRED

Authenticated

METHOD OF DISCOVERY

Automated

METHOD OF EXPLOITATION

Manual

The target system analysis visualizes the scope of the security assessment and provides a high-level overview of the target's attack surface and functionalities as seen from the attacker's perspective.

[illegible]