RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

Security Industry Call-to-Action: We Need a Cloud Vulnerability Database

Ami Luttwak
CTO & CO-FOUNDER
WIZ
@amiluttwak

John Yeoh
EVP, Global Research
CSA
@YoTheShow

Pete Chronis
SVP, CISO
Paramount (ViacomCBS)
@chronis

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.

Outline

- Vulnerabilities in the pre-cloud era
- A new type of cloud vulnerabilities
- Examples / Use cases
- Solution proposal
- What can we do as a community to solve the cloud vulnerabilities issue?

Who are we?

Ami Luttwak

CTO & CO-FOUNDER
WIZ

John Yeoh

Global VP, Research
Cloud Security Alliance

Pete Chronis

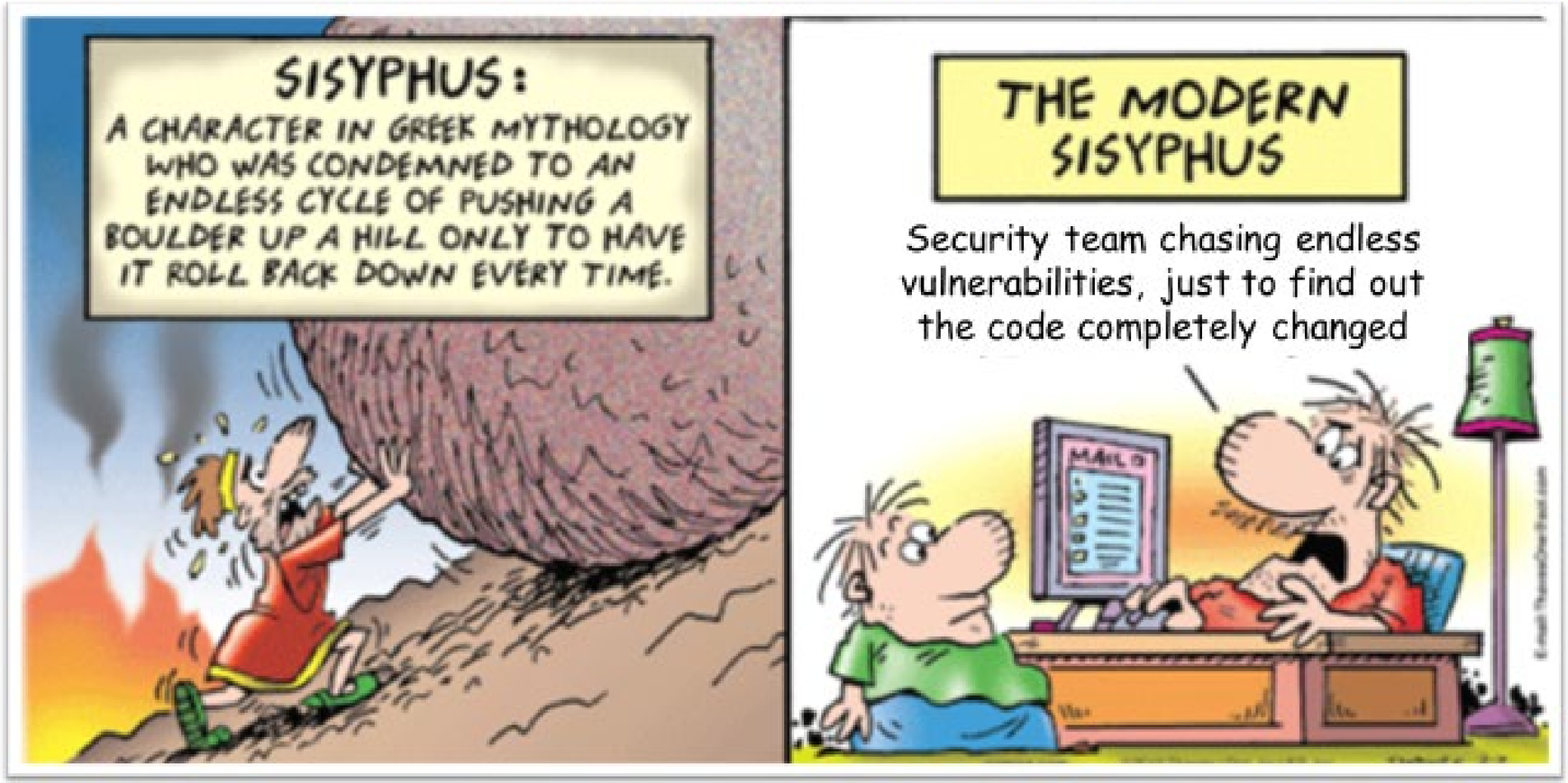
SVP, CISO
Paramount (ViacomCBS)

Wiz Research: Breaking the cloud

- Experienced cloud researchers
- Identified the most influential cloud vulnerabilities in recent months : #CHAOSDB, #OMIGOD, #ExtraReplica

Recent Publications

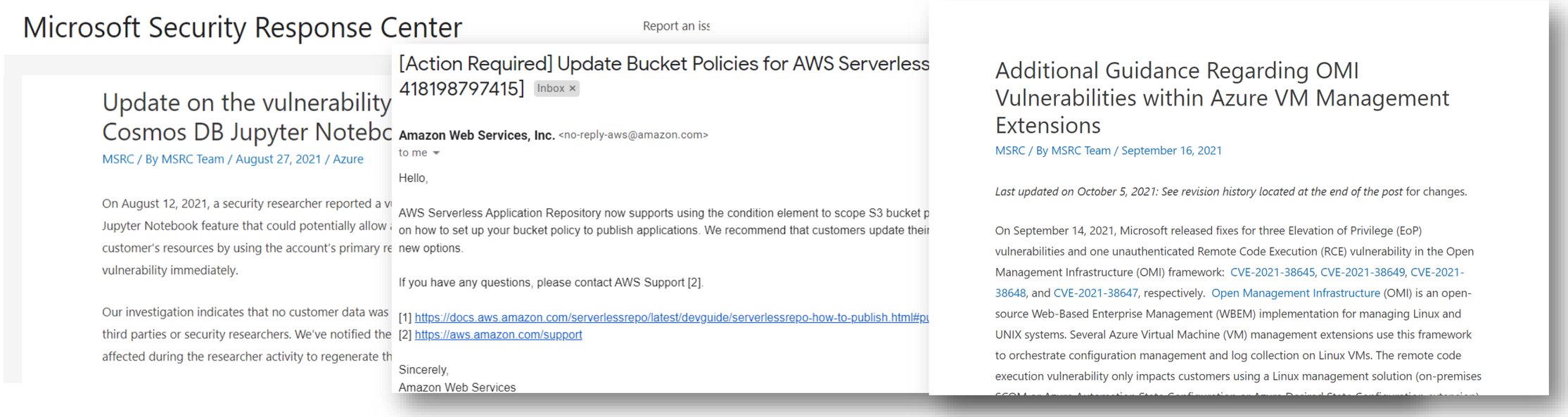
A Day In The Life of Security: An Endless Pursuit



Wiz Kickoff 2022

Introduction:
A day in a CISO's life

- How do you ensure your organization is protected from software vulnerabilities?
- How do you ensure your organization is protected from cloud vulnerabilities?



Introduction:
Security in the pre-cloud era

Users are fully responsible for their security:

- Hardware
- Network
- Servers
- Identities
- And everything else…

Introduction:
Security in the cloud

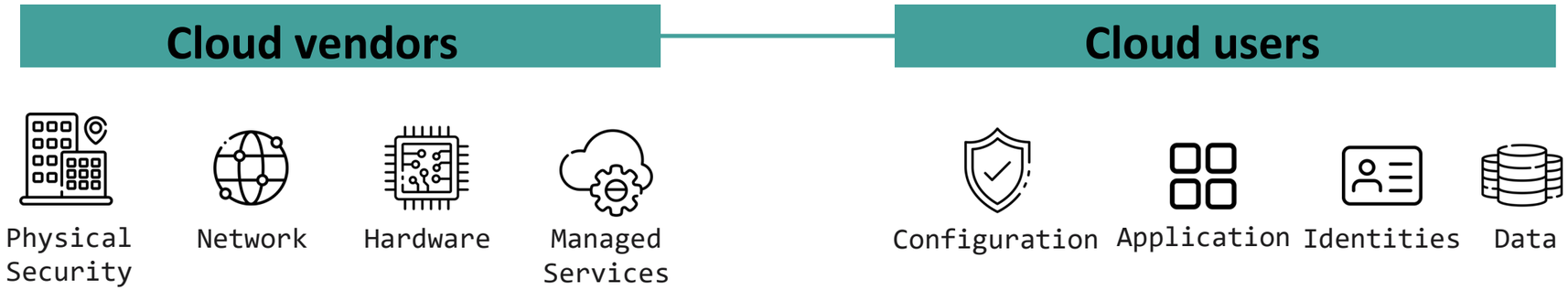
Cloud vendors:

- Physical Security
- Servers
- Network
- Hardware
- Managed Services
- Storage

Cloud users:

- Application (CVEs)
- Configuration
- Identities
- Data

Introduction:
the Shared Responsibility Model



The Problem:
Cloud vulnerabilities are different

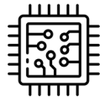
- **New types of vulnerabilities:** (not software)
  - Configuration vulnerabilities
  - Identity vulnerabilities
- **Software owned by the cloud provider**
  - No software version
  - No defined patching process
- **Complex remediation steps**

Cracks in the Shared Responsibility Model

Cloud vendors — **New cloud issues** — **Cloud users**


Physical Security


Network


Hardware


Managed Services


Configuration

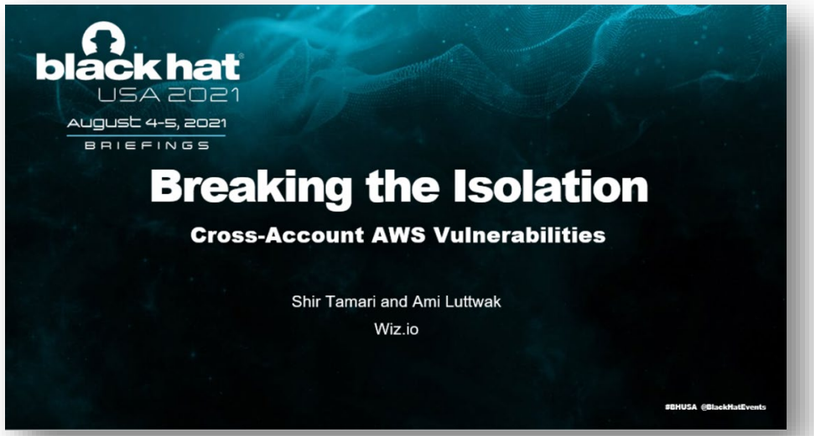

Application

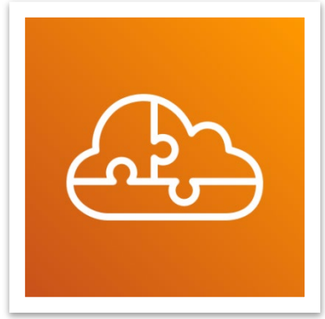

Identities


Data

Example #1: Vulnerable Configuration
The issue

- Multiple AWS services found vulnerable
- Read/Write to cross-tenant resources
- Default access policies were vulnerable





Serverless Repo

AWS CloudTrail

AWS Config

AWS Guard Duty

Example #1: Vulnerable Configuration
The issue

```
{
  "Effect": "Allow",
  "Principal": {"Service": "serverlessrepo.amazonaws.com"},
  "Action": "s3:GetObject",
  "Resource": "arn:aws:s3:::bucketname/*"
}
```

Mitigations:

Cloud Provider Remediation

- AWS added scoping conditions to their policies
- Updated the documentation

But what about vulnerable customers?

- Alerted vulnerable customers via email
- Alerted vulnerable customers on the AWS Personal Health Dashboard

Mitigations:

Vulnerable AWS Configurations

[Action Required] Update Bucket Policies for AWS Serverless Application Repository [AWS Account: [redacted]] Inbox ×

Amazon Web Services, Inc. <no-reply-aws@amazon.com> Wed, Feb 3, 3:21 AM

to me

Hello,

AWS Serverless Application Repository now supports using the condition element to scope S3 bucket policies to specific AWS accounts. Please refer to our documentation[1] for more information on how to set up your bucket policy to publish applications. We recommend that customers update their existing bucket policies used with the Serverless Application Repository to utilize these new options.

If you have any questions, please contact AWS Support [2].

[1] https://docs.aws.amazon.com/serverlessrepo/latest/devguide/serverlessrepo-how-to-publish.html#publishing-application-through-aws-console
[2] https://aws.amazon.com/support

Sincerely,
Amazon Web Services

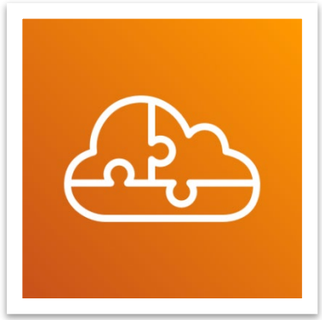
Amazon Web Services, Inc. is a subsidiary of Amazon.com, Inc. Amazon.com is a registered trademark of Amazon.com, Inc. This message was produced and distributed by Amazon Web Services Inc., 410 Terry Ave. North, Seattle, WA 98109-5210

Reference: https://phd.aws.amazon.com/phd/home#/event-log?Event%20ARN=arn:aws:health:global::event/SERVERLESSREPO/AWS_SERVERLESSR

[redacted]

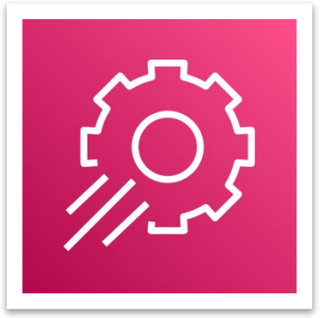
Example #1: Vulnerable Configuration
Users own the remediation

- 90% of orgs were still vulnerable 5 months after the notification
- AWS cannot update users' policies
- Users must do it themselves



Serverless Repo

AWS CloudTrail



AWS Config

AWS Guard Duty

Takeaways

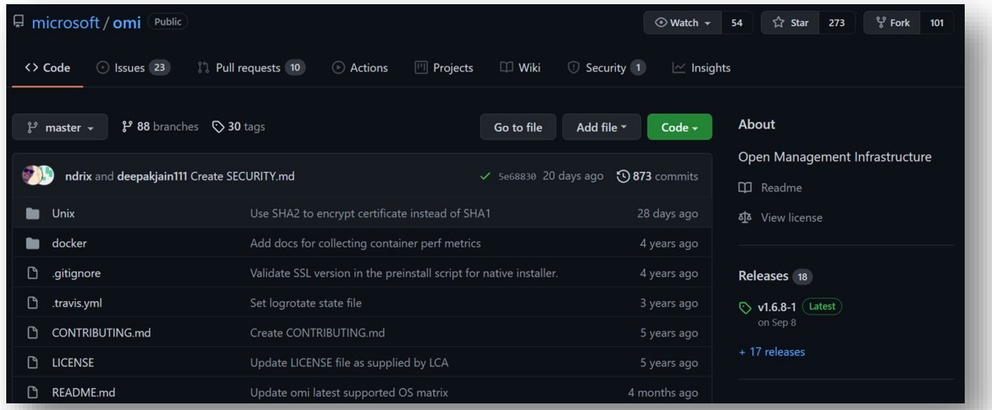
Breaking the isolation: cross-account AWS vulnerabilities

- No standard notification channel
- No identification of the issue
- No tracking system
- No Severity scoring
- Mitigating cloud vulnerabilities process does not exist!
- **The result: Most cloud user are still vulnerable!**

Example #2: Cloud middleware

The issue

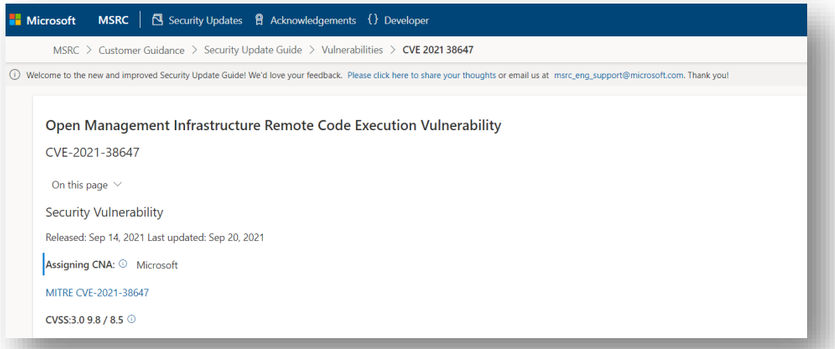
- OMI is a cloud middleware used by many Azure services
- Silently installed on customers virtual machines!
- Wiz found 4 vulnerabilities in OMI (dubbed OMIGOD) enabling a remote attacker to execute code with root privileges
- Thousands of customer are at risk



Example #2: Cloud middleware

CSP Remediation

- Microsoft published it on September ‘21 Patch Tuesday
- 1 Remote Code Execution, 3 Local Privilege Escalation
- Critical/High severity
- Provided guidance to customers on updating the agent
- Customers should apply the patch themselves, even though they are not aware of it.



Example #2: Cloud middleware

CSP Remediation

- Microsoft published it on September ‘21 Patch Tuesday
- 1 Remote Code Exe[illegible] Escalation
- Critical/High severit[illegible]
- Provided[illegible]t
- Custome[illegible]hough they are not aware of it.

Kevin Beaumont
@GossiTheDog

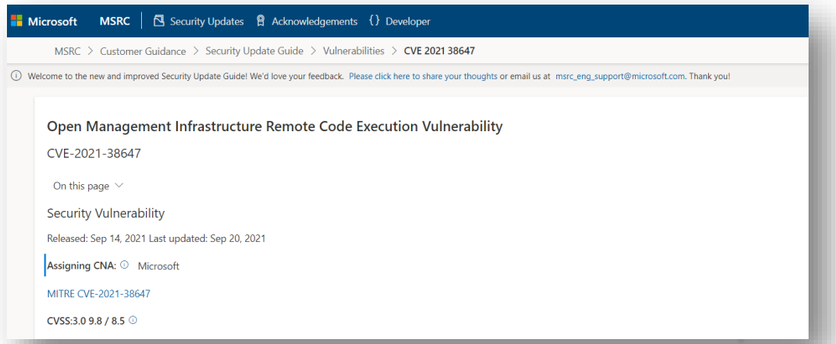
Microsoft Azure silently install management agents on your Linux VMs, which now have RCE and LPE vulns.

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

2,559 Retweets 532 Quote Tweets 4,339 Likes

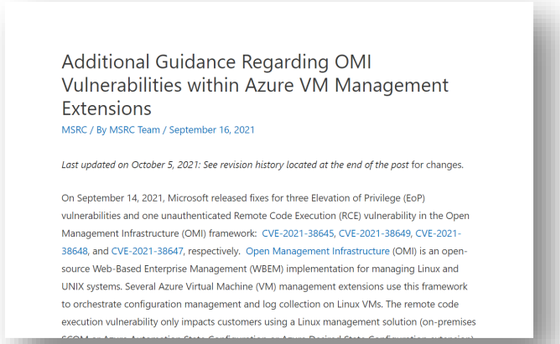


Example #2: Cloud middleware

CSP remediation gaps

- The software vulnerability impacted multiple services LogAnalytics, Azure Automation, Azure Sentinel..
- Insufficient notification :

The CVE was issued for OMI, customers are not aware of OMI (undocumented)



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.

On September 14, 2021, Microsoft released fixes for three Elevation of Privilege (EoP) vulnerabilities and one unauthenticated Remote Code Execution (RCE) vulnerability in the Open Management Infrastructure (OMI) framework: CVE-2021-38645, CVE-2021-38649, CVE-2021-38648, and CVE-2021-38647, respectively. Open Management Infrastructure (OMI) is an open-source Web-Based Enterprise Management (WBEM) implementation for managing Linux and UNIX systems. Several Azure Virtual Machine (VM) management extensions use this framework to orchestrate configuration management and log collection on Linux VMs. The remote code execution vulnerability only impacts customers using a Linux management solution (on-premises

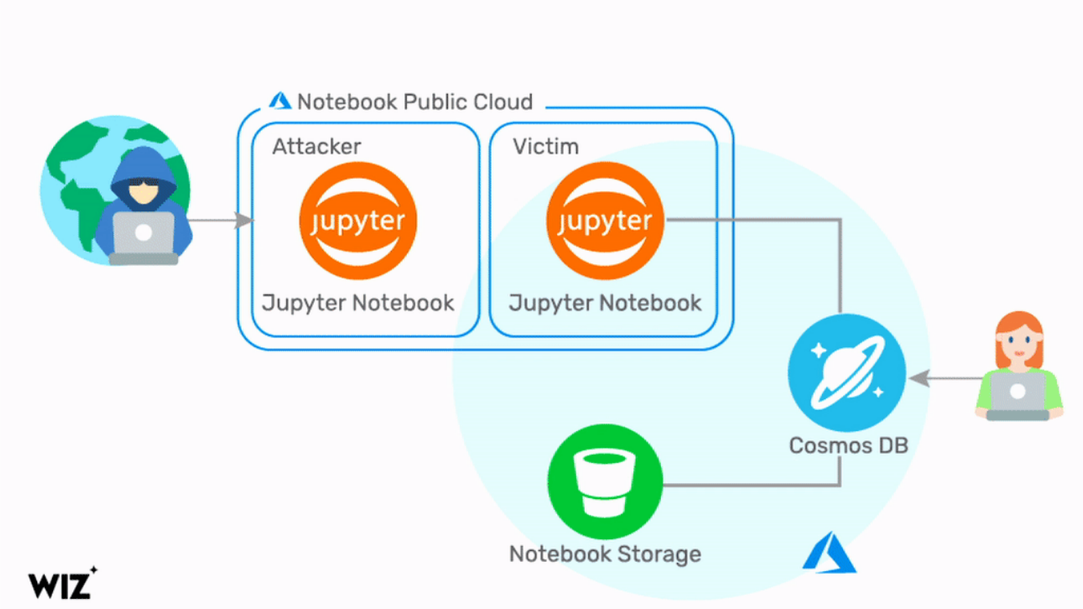
Key Takeaways:

OMIGOD! Multiple Vulnerabilities In Azure's OMI Agent

- Vulnerabilities can be found in pre-installed middleware
- No identification -It's not only a software vulnerability; multiple Azure services were affected
- Lack of transparency- customers didnt know which Azure services use the agent
- No tracking system
- No remediation – Microsoft shared details on the affected Azure services remediation 2 days after Patch Tuesday

Example #3: Key Leak
The issue

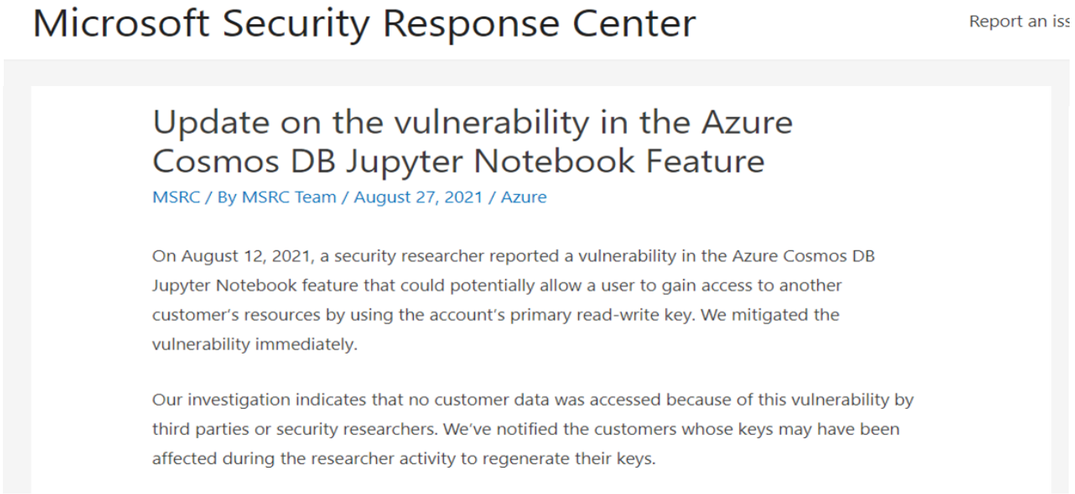
- On August 2021, unprecedented cloud cross-account vulnerability in Azure Cosmos DB
- Access keys were leaked, and risked thousands of customers



Example #3: Key Leak

CSP Remediation

- Access keys must be regenerated by Cosmos DB customers
- Microsoft emailed selected customers and later published a blog post
- The service vulnerability timeframe isn’t clear



Microsoft Security Response Center

Report an iss

Update on the vulnerability in the Azure Cosmos DB Jupyter Notebook Feature

MSRC / By MSRC Team / August 27, 2021 / Azure

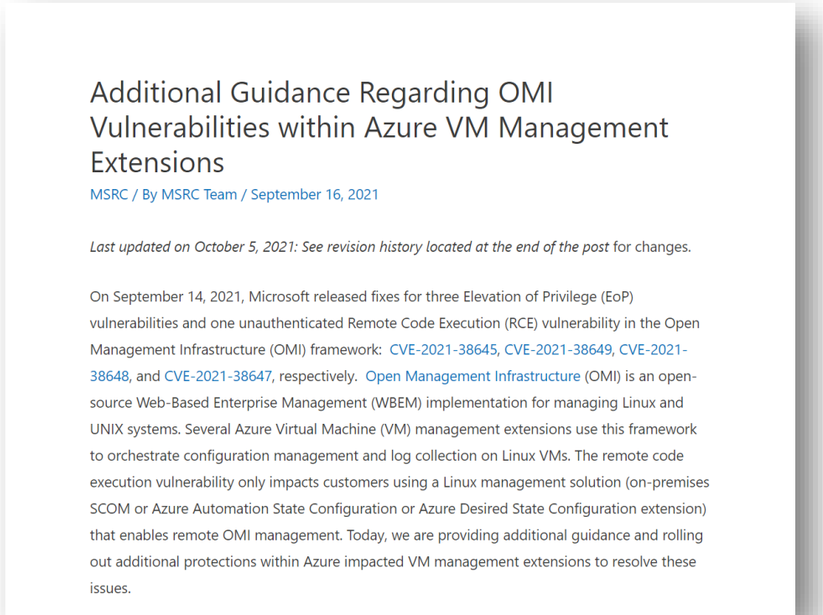
On August 12, 2021, a security researcher reported a vulnerability in the Azure Cosmos DB Jupyter Notebook feature that could potentially allow a user to gain access to another customer’s resources by using the account’s primary read-write key. We mitigated the vulnerability immediately.

Our investigation indicates that no customer data was accessed because of this vulnerability by third parties or security researchers. We’ve notified the customers whose keys may have been affected during the researcher activity to regenerate their keys.

Key Takeaways:

ChaosDB : Cross-account vulnerability in Azure Cosmos DB

- Vulnerability fix can be both CSP and customer responsibility
- No identification –No unique id to the issue
- No tracking system – notification was sent only in mail
- Lack of transparency - Microsoft didn’t plan to publish its blog, vulnerability timeframe is missing



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.

On September 14, 2021, Microsoft released fixes for three Elevation of Privilege (EoP) vulnerabilities and one unauthenticated Remote Code Execution (RCE) vulnerability in the Open Management Infrastructure (OMI) framework: CVE-2021-38645, CVE-2021-38649, CVE-2021-38648, and CVE-2021-38647, respectively. Open Management Infrastructure (OMI) is an open-source Web-Based Enterprise Management (WBEM) implementation for managing Linux and UNIX systems. Several Azure Virtual Machine (VM) management extensions use this framework to orchestrate configuration management and log collection on Linux VMs. The remote code execution vulnerability only impacts customers using a Linux management solution (on-premises SCOM or Azure Automation State Configuration or Azure Desired State Configuration extension) that enables remote OMI management. Today, we are providing additional guidance and rolling out additional protections within Azure impacted VM management extensions to resolve these issues.

Summary

The Shared Responsibility Model is broken

- No standard notification channel
- Issues cannot be tracked easily
- No severity scoring – how should we prioritize?
- Lack of transparency

Conclusions

- Vulnerabilities are not only in code / software

We lack for cloud vulnerabilities:

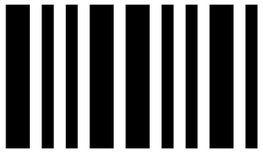
- Identification
- Tracking system
- Transparency
- Severity Standardization
- Remediation steps

Reporting & enumeration for Cloud Vulnerabilities

What's missing?

- Centralized database
- Public, used by cloud users and security vendors
- Vulnerabilities should be reported by cloud service providers

Example ChaosDB: Identification



- Identifier: Cloud Vulnerability 2021-1337

Example ChaosDB: Severity

- Identifier: Cloud Vulnerability 2021-1337
- Severity: Critical

Example ChaosDB: Transparency

- Identifier: Cloud Vulnerability 2021-1337
- Severity: Critical
- Product/Platform: Azure Cosmos DB
- Time affected: 02/01/2021 – 08/12/2021
- Risk: The vulnerability could allow a user to gain access to another customer's resources by using the account's primary read-write key

Example ChaosDB: Remediation

- Identifier: Cloud Vulnerability 2021-1337
- Product/Platform: Azure Cosmos DB
- Severity: Critical
- Time affected: 02/01/2021 – 08/12/2021
- Risk: The vulnerability could allow a user to gain access to another customer's resources by using the account's primary read-write key
- Required Action: Regenerate the primary read-write key for each of the impacted Azure Cosmos DB

Example ChaosDB: Tracking

- Identifier: Cloud Vulnerability 2021-1337
- Product/Platform: Azure Cosmos DB
- Severity: Critical
- Time affected: 02/01/2021 – 08/12/2021
- Risk: The vulnerability could allow a user to gain access to another customer's resources by using the account's primary read-write key
- Required Action: Regenerate the primary read-write key for each of the impacted Azure Cosmos DB
- Detection: See attached Rego rule

Example ChaosDB:

Identifier	Cloud Vulnerability 2021-1337
Product/Platform	Azure Cosmos DB
Severity	Critical
Time period	02/01/2021 - 08/12/2021
Risk	The vulnerability could allow a user to gain access to another customer's resources by using the account's primary read-write key
Required actions	Regenerate the primary read-write key for each of the impacted Azure Cosmos DBs
Detection method	See attached Rego rule

Auditing Your Environment with the New Cloud Database

Identifier	Description	Platform	Date
2021-1337	Action Required: Regenerate Azure Cosmos DB Keys	Azure Cosmos DB	08/12/2021
2021-1338	OMI Vulnerabilities within Azure VM Management Extensions	Azure Log analytics, Azure Automation	09/14/2021
2021- 1339			
2021-1240			
2021-1341			

Tracking Vulnerabilities

History and evolution

- Bug hunting in mailing lists to CVE and CERT – pre-1999
- OSV, NVD, and other vendor platforms – a lot more today

Technology

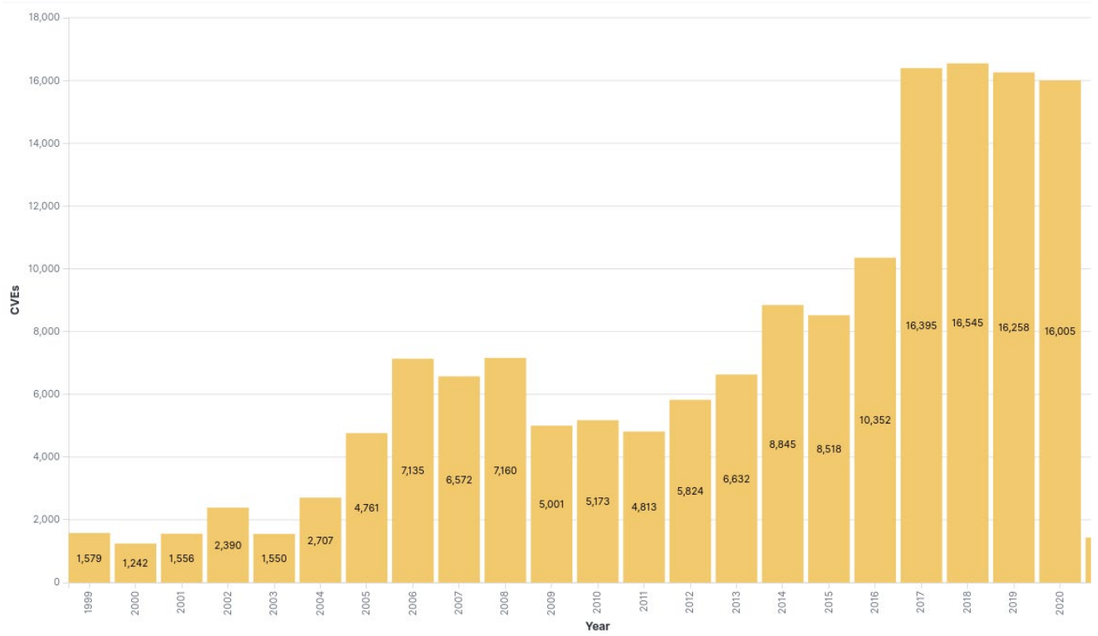
Continues to grown and evolve faster than vulnerability identification

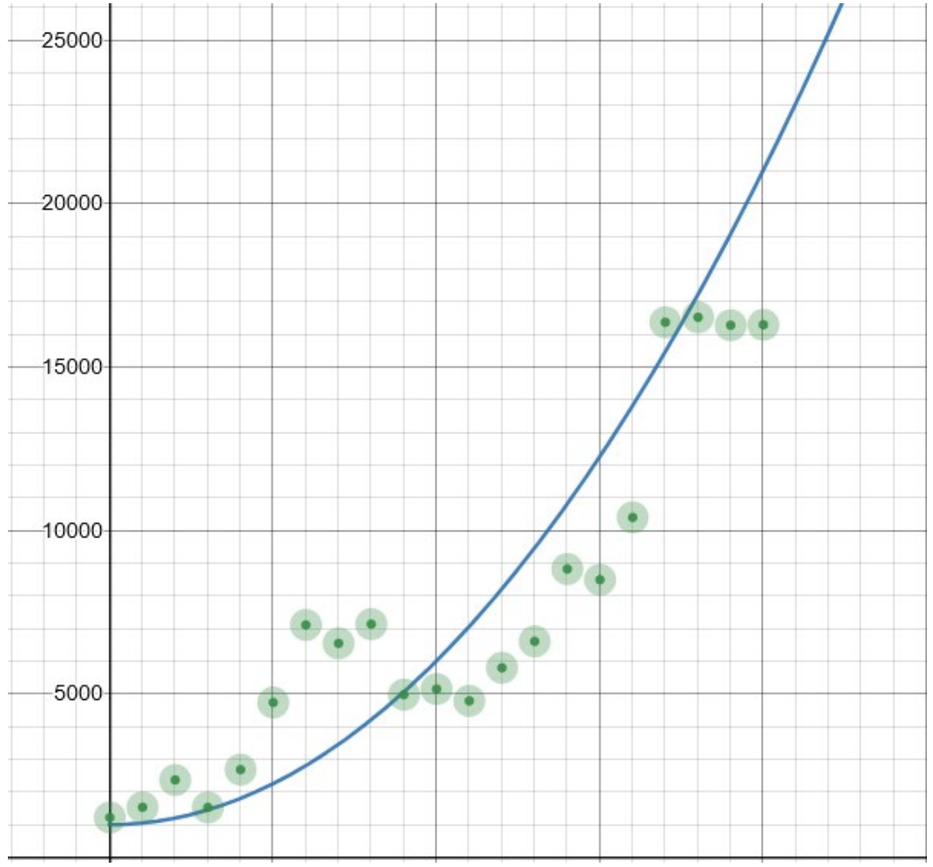
- The use of Cloud
- The use of 3rd party services
- Build vs. Buy is being challenged
- Outpacing how we identify
- Difficult to disclose
- Too much is unseen

Keeping Pace

Current limitations

- CVE identification trends





What is Needed

- Speed to identify, protect, recover
  - Automate and consolidate
- Inclusivity for today's IT
  - IT environment - software, hardware, services (cloud), configurations, documentation
  - Customer and third-party owned
  - IT stakeholders - researchers, providers, customers, authorities, etc.
- Examples
  - Where are the vulnerabilities
  - Areas of impact
  - Mitigate and remediate

A day in CISO's life

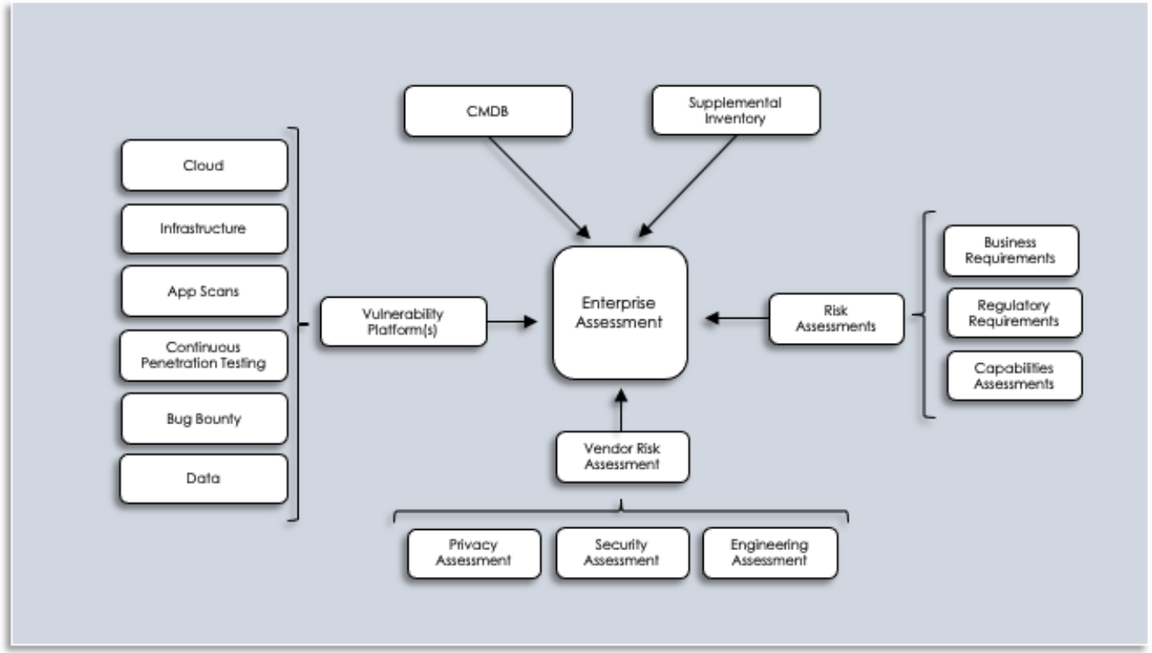
and now with the Cloud Vulneraility DB

- How would a new CISO day look like:

A day in CISO's life

and now with the Cloud Vulneraility DB

- Unified Risk Management View

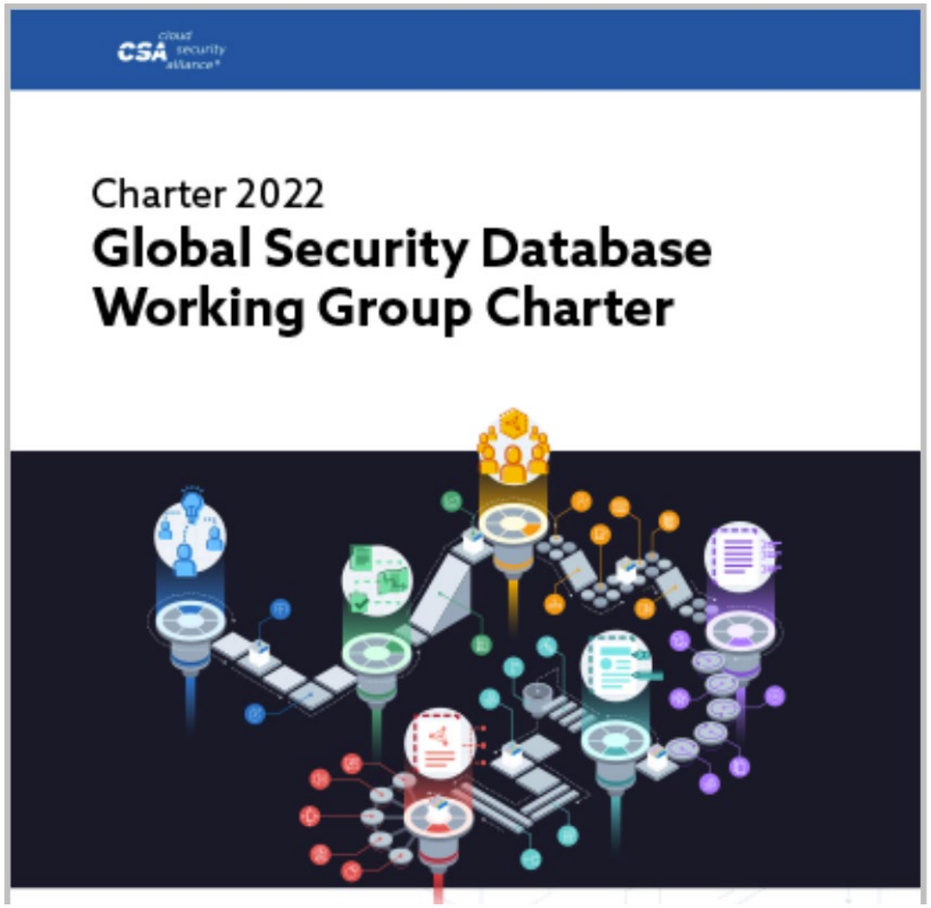


What's next?

Solutions

- Community-driven
  - Inclusive of all stakeholders
  - Community over committee
- Database
  - Built for speed; automation, community-driven
- Centralized and inclusive
  - Template for all existing identifiers; CVE, NVD, CWE, vendors
- Discoverable
  - Scrape the internet; social

CSA Initiative: Global Security Database



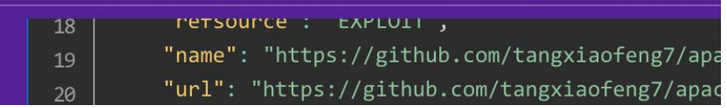
Global Security Database

globalsecuritydatabase.org

- Open Source
- Community, not committee
- Common place, multiple viewpoints
- Machine-first, automation
- Using existing formats where possible
- Ingest other databases

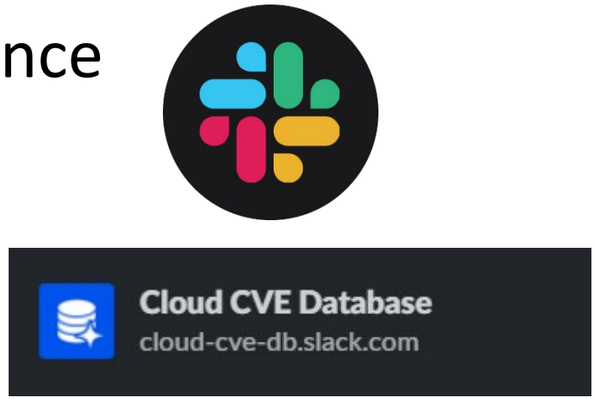
GSD

Key	
id	GSD-2021-1002352
vendor_name	Apache
product_name	• Log4j • Log4j2
product_version	<=2.14.1
vulnerability_type	• CWE-502 Deserialization of Untrusted Data • CWE-400 Uncontrolled Resource Consumption • CWE-20 Improper Input Validation
affected_component	unspecified
attack_vector	network
impact	remote code execution
credit	



Cloud CVE Database: Our community

- A group of people that want to create a better future for all cloud users and providers
- 130+ members
- From different companies, including Fortune500
- 12 different time zones
- Diverse backgrounds as finance, security, data, compliance
- Join us: bit.ly/cloudVuln



A new DB to centralize all cloud security issues

- A central location for all cloud security issues from all CSPs
- Moderated by the community

Other community projects & partners

- The Cloud Security Notification Framework (CSNF)
- MITRE’s CVE

How can we make the change happen?

- Industry action - call the CSPs to provide for each new cloud vulnerability:
- Identification
- Tracking system
- Transparency
- Severity Standardization
- Remediation steps

Call for action:

The shared responsibility model is broken

The power is in your hands!

Thank you

Read more on:

https://globalsecuritydatabase.org/

wiz.io/blog

Join our slack group:

bit.ly/cloudVuln

Follow us

@amiluttwak

@chronis

@yotheshow