HC3: Sector Alert

June 07, 2024 TLP:CLEAR Report: 202406071200

Prevention of Unauthorized Access for Snowflake

Executive Summary

On June 02, 2024, Snowflake observed an increase in cyber threats targeting accounts on their cloud data platform. The vulnerability is possibly associated with CVE-2023-51662. HC3 strongly encourages all users to review the following advisory, and to apply any mitigations to prevent serious damage from occurring to the Healthcare and Public Health (HPH) sector.

Report

Snowflake has recently detected and is investigating an uptick in cyber threats targeting certain customer accounts. The manufacturer suspects this is due to ongoing, industry-wide, identity-based attacks to access customer data. Additional research suggests that these attacks use user credentials that are exposed through unrelated cyber incidents. It is not believed that this activity is linked to any vulnerability, misconfiguration, or malicious activity within the Snowflake product, but may be related to CVE-2023-51662.

Detailed information on preventing any possible threat activity within Snowflake accounts and on disabling these malicious accounts can be viewed here.

It should be noted that, if the ALLOW_ID_TOKEN parameter is enabled on your account, you must keep the user disabled for six hours to fully invalidate any potential unauthorized access through this ID token feature. Re-enabling the user before this period ends could allow an attacker to generate a new session using an existing ID token, even if the password has been reset or if MFA has been enabled. After deactivating the account, Snowflake recommends contacting the account owner to verify if the activity originated from them.

Snowflake is investigating activity from the following IP addresses:

- 104.223.91.28
- 198.54.135.99
- 184.147.100.29
- 146.70.117.210
- 198.54.130.153
- 169.150.203.22
- 185.156.46.163
- 146.70.171.99
- 206.217.206.108
- 45.86.221.146
- 193.32.126.233
- 87.249.134.11
- 66.115.189.247
- 104.129.24.124
- 146.70.171.112
- 198.54.135.67
- 146.70.124.216
- 45.134.142.200
- 206.217.205.49
- 146.70.117.56
- 169.150.201.25
- 66.63.167.147
- 194.230.144.126
- 146.70.165.227
- 154.47.30.137
- 154.47.30.150
- 96.44.191.140
- 146.70.166.176
- 198.44.136.56
- 176.123.6.193
- 192.252.212.60
- 173.44.63.112
- 37.19.210.34
- 37.19.210.21
- 185.213.155.241
- 198.44.136.82
- 93.115.0.49
- 204.152.216.105

- 198.44.129.82
- 185.248.85.59
- 198.54.131.152
- 102.165.16.161
- 185.156.46.144
- 45.134.140.144
- 198.54.135.35
- 176.123.3.132
- 185.248.85.14
- 169.150.223.208
- 162.33.177.32
- 194.230.145.67
- 5.47.87.202
- 194.230.160.5
- 194.230.147.127
- 176.220.186.152
- 194.230.160.237
- 194.230.158.178
- 194.230.145.76
- 45.155.91.99
- 194.230.158.107
- 194.230.148.99
- 194.230.144.50
- 185.204.1.178
- 79.127.217.44
- 104.129.24.115
- 146.70.119.24
- 138.199.34.144
- 198.44.136.35
- 66.115.189.210
- 206.217.206.88
- 37.19.210.28
- 146.70.225.67
- 138.199.43.92
- 149.102.246.3
- 43.225.189.163
- 185.201.188.34
- 178.249.209.163
- 199.116.118.210
- 198.54.130.147
- 156.59.50.195
- 198.44.136.195
- 198.44.129.67
- 37.19.221.170
- 96.44.189.99
- 146.70.134.3
- 66.115.189.200
- 103.75.11.51
- 69.4.234.118
- 146.70.173.195
- 138.199.60.29
- 66.115.189.160
- 154.47.30.144
- 178.249.211.80
- 143.244.47.92
- 146.70.132.227
- 193.19.207.226
- 46.19.136.227
- 68.235.44.35
- 103.136.147.4
- 198.54.133.163
- 169.150.203.16
- 146.70.224.3
- 87.249.134.15
- 198.54.134.131
- 142.147.89.226
- 146.70.117.35
- 193.19.207.196
- 146.70.144.35
- 146.70.173.131
- 107.150.22.3
- 169.150.201.29
- 146.70.117.163
- 146.70.138.195
- 146.70.184.67
- 104.129.57.67
- 185.248.85.49
- 146.70.168.67
- 138.199.43.66
- 79.127.217.35
- 194.127.167.108
- 194.36.25.49
- 146.70.171.67
- 138.199.60.3
- 45.134.212.93
- 146.70.187.67
- 66.63.167.163
- 154.47.29.3
- 149.102.246.16
- 198.44.129.99
- 146.70.128.195
- 185.65.134.191

- 146.70.119.35
- 87.249.134.28
- 149.102.240.67
- 103.75.11.67
- 69.4.234.124
- 169.150.196.3
- 169.150.201.3
- 185.188.61.196
- 87.249.134.2
- 138.199.15.163
- 45.134.213.195
- 138.199.6.208
- 169.150.227.223
- 146.70.200.3
- 149.88.22.156
- 173.205.85.35
- 206.217.206.48
- 194.36.25.4
- 154.47.16.48
- 37.19.200.131
- 146.70.166.131
- 37.19.221.144
- 149.88.20.207
- 79.127.222.195
- 194.127.167.88
- 96.44.191.131
- 69.4.234.119
- 138.199.6.221
- 146.70.128.227
- 66.63.167.195
- 169.150.196.16
- 185.201.188.4
- 173.44.63.67
- 79.127.222.208
- 198.54.134.99
- 198.54.135.131
- 138.199.43.79
- 66.115.189.190
- 149.88.20.194
- 141.98.252.190
- 129.227.46.163
- 31.171.154.51
- 79.127.217.48
- 69.4.234.116
- 206.217.206.68
- 103.125.233.19
- 146.70.188.131
- 169.150.227.198
- 129.227.46.131
- 198.44.136.99
- 149.88.22.130
- 193.138.7.138
- 146.70.168.195
- 169.150.203.29
- 206.217.205.118
- 146.70.185.3
- 146.70.124.131
- 194.127.199.32
- 149.102.240.80
- 143.244.47.79
- 178.255.149.166
- 188.241.176.195
- 69.4.234.125
- 138.199.21.240
- 45.134.79.98
- 178.249.209.176
- 68.235.44.3
- 198.54.133.131
- 193.138.7.158
- 154.47.30.131
- 204.152.216.115
- 206.217.205.125
- 37.19.200.144
- 146.70.171.131
- 198.54.130.99
- 149.22.81.208
- 146.70.197.131
- 198.54.131.131
- 138.199.15.147
- 185.248.85.34
- 143.244.47.66
- 92.60.40.225
- 178.249.214.3
- 146.70.133.3
- 179.43.189.67
- 69.4.234.120
- 146.70.199.195
- 185.156.46.157
- 45.134.142.194
- 68.235.44.195
- 209.54.101.131
- 104.129.41.195

- 146.70.225.3
- 206.217.205.126
- 103.136.147.130
- 194.110.115.3
- 178.249.211.93
- 185.188.61.226
- 194.110.115.35
- 146.70.198.195
- 169.150.198.67
- 103.108.229.67
- 138.199.60.16
- 96.44.191.147
- 31.170.22.16
- 45.134.140.131
- 169.150.196.29
- 103.216.220.19
- 173.205.93.3
- 146.70.199.131
- 103.214.20.131
- 149.88.22.143
- 149.40.50.113
- 138.199.21.227
- 138.199.6.195
- 103.216.220.35
- 198.44.136.67
- 199.116.118.194
- 146.70.129.131
- 199.116.118.233
- 146.70.184.3
- 185.254.75.14
- 38.240.225.69
- 149.22.81.195
- 43.225.189.132
- 45.134.142.207
- 146.70.196.195
- 198.44.140.195
- 206.217.205.119
- 38.240.225.37
- 169.150.227.211
- 37.19.200.157
- 146.70.132.195
- 146.70.211.67
- 206.217.206.28
- 178.249.214.16
- 149.88.22.169
- 149.88.104.16
- 194.36.25.34
- 146.70.197.195
- 45.134.212.80
- 156.59.50.227
- 104.223.91.19
- 198.54.130.131
- 185.248.85.19
- 45.134.79.68
- 45.134.142.220
- 185.204.1.179
- 146.70.129.99
- 146.70.133.99
- 69.4.234.122
- 178.249.211.67
- 198.54.131.163
- 198.44.129.35
- 103.108.231.51
- 146.70.165.3
- 37.19.221.157
- 92.60.40.210
- 154.47.16.35
- 194.127.199.3
- 37.19.210.2
- 103.108.231.67
- 204.152.216.99
- 176.123.7.143
- 176.123.10.35
- 195.160.223.23

In addition to the above IP addresses, the manufacturer has also observed malicious traffic from clients with the following characteristics:

- Connections from a client identifying itself as rapeflake.
- Connections from a client identifying itself as DBeaver_DBeaverUltimate and running from Windows Server 2022

References

Snowflake. Detecting and Preventing Unauthorized User Access: Instructions. June 03, 2024. Detecting

and Preventing Unauthorized User Access: Instructions (snowflake.com)

NIST. CVE-2023-51662. January 03, 2024. NVD - CVE-2023-51662 (nist.gov)

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback