09 August 2024

MCB 02-24: Threat Actors Targeting Amazon Web Services (AWS) Simple Storage Service (S3) Vulnerability

THREAT SUMMARY

Ransomware actors continue to target the Marine Transportation System (MTS), and they may be getting more creative. Recently, an unknown threat actor targeted an MTS entity's AWS server that was used to store company data. The threat actor accessed the server, erased its contents, and left a ransom note stating they had exfiltrated the data. They went on to threaten to make the exfiltrated information public if they did not receive a ransom payment. While the threat actor did delete the data stored on the server, further investigation by the MTS entity revealed the threat actor never exfiltrated information from the compromised server. Rather, they claimed they had exfiltrated sensitive data to increase pressure on the victim, in an attempt to convince them to pay the ransom. This attack took advantage of an AWS S3 bucket misconfiguration, documented as CVE-2022-31159. Publicly-accessible misconfigured buckets can be found by threat actors using tools such as S3Scanner and S3Finder, which may be exploited in a similar manner as the case described above.

Recommendations

MTS entities that use AWS S3 Buckets are encouraged to configure buckets to not be publicly available. Additionally, ensure the AWS S3 TransferManager component of the AWS Software Development Kit for Java v1 is properly patched to a minimum version of 1.12.261 in accordance with CVE-2022-31159. MTS entities are reminded to follow CISA's best practices to mitigate the chances of suffering a ransomware attack.

- #StopRansomware Guide

Sources

NIST National Vulnerability Database. https://nvd.nist.gov/vuln/detail/CVE-2022-31159

Configuration and Vulnerability Analysis in Amazon S3, https://docs.aws.amazon.com/AmazonS3/latest/userguide/vulnerability-analysis-and-management.html

CISA Cyber Security Best Practices, https://www.cisa.gov/resources-tools/

Resources

Facilities that observe any unusual activity or interruptions to their network should report those activities per Navigation and Vessel Inspection Circular (NVIC) 02-24 to:

Coast Guard's National Response Center
1-800-424-8802

OR

Cybersecurity and Infrastructure Security Agency (CISA) Central
1-888-282-0870

If you have any questions, please visit our website at:
https://www.uscg.mil/MaritimeCyber
or reach out to MCRB at:
maritimecyber@uscg.mil