Cyber Threat Intelligence

CRITICALSTART® Threat Research

Cloud Development Kit (CDK) Attack

Incident Summary

The CDK (Cloud Development Kit) attack represents a significant threat vector targeting AWS Cloud Development Kit (AWS CDK) users. AWS CDK is a widely used framework for defining cloud infrastructure through code, which translates into AWS CloudFormation templates for provisioning.

Attack Vector Analysis

1. Code Injection: Malicious actors may inject unauthorized code into CDK scripts. This can lead to unintended infrastructure changes, which could include the deployment of compromised resources or opening backdoors.
2. Misconfiguration Exploitation: Vulnerabilities arising from misconfigurations within CDK scripts can be exploited. Attackers might leverage these flaws to gain unauthorized access or escalate their privileges within the cloud environment.
3. Supply Chain Attacks: Attackers could target dependencies and libraries used by CDK. By compromising these elements, they introduce vulnerabilities or malicious code into the infrastructure definitions, potentially affecting multiple deployments.
4. Insider Threats: Employees or contractors with legitimate access to CDK scripts could intentionally introduce malicious modifications. These changes might go unnoticed until the compromised infrastructure is deployed.
5. IAM Misconfigurations: Improperly configured Identity and Access Management (IAM) policies in CDK scripts could grant excessive permissions, which attackers could exploit to gain broader access for lateral movement within the cloud environment.

Mitigation Strategies

To mitigate the risks associated with CDK attacks, organizations should consider the following actions:

- Code Review and Audits: Conduct regular thorough reviews and audits of CDK scripts to identify and remediate potential vulnerabilities.
- Access Controls: Implement strict access controls and enforce the principle of least privilege (PoLP) to limit access to CDK scripts and the resulting cloud infrastructure.
- Automated Scanning: Use automated tools to continuously scan for vulnerabilities and misconfigurations in CDK scripts.
- Dependency Management: Regularly update dependencies and libraries to patch known vulnerabilities to minimize the risk of supply chain attacks.
- Monitoring and Logging: Implement robust monitoring and logging mechanisms to track changes to CDK scripts and infrastructure deployments.

Intelligence Insights

This attack vector highlights the importance of securing infrastructure-as-code (IaC) environments. With the increasing adoption of IaC frameworks like AWS CDK, threat actors are likely to target these systems to exploit their vulnerabilities.

Organizations must stay vigilant and proactive in safeguarding their cloud environments by continuously evolving their security practices and integrating intelligence insights into their defense strategies.

Future Monitoring

Continuous monitoring and intelligence gathering on CDK-related threats are crucial. Threat intelligence teams should keep an eye on emerging attack techniques targeting IaC frameworks and adjust their defense mechanisms accordingly. Collaboration with security operation centers (SOC) and security engineering teams will be essential to implement relevant detections and responses promptly.

Conclusion

The CDK attack underscores the evolving threat landscape in cloud security. As organizations increasingly rely on IaC frameworks for efficient cloud management, they must also prioritize securing these environments against sophisticated threat actors. By implementing a blend of proactive security measures and continuous monitoring, organizations can better defend against potential CDK attacks.

The CRITICALSTART® Cyber Research Unit will continue to monitor the situation and work closely with the SOC and Security Engineering team to implement any relevant detections. For future updates the CTI team will post updates via Cyber Operations Risk & Response™ Bulletins and on the CRITICALSTART® Intelligence Hub.

References

1. https://docs.aws.amazon.com/cdk/v2/guide/security.html
2. https://dev.to
3. https://aws.amazon.com/blogs/apn/shift-left-security-in-infrastructure-as-code-using-aws-cdk-and-checkmarx-kics/
4. https://rhinosecuritylabs.com
5. https://live.paloaltonetworks.com