LocalStack zero-day vulnerabilities chained to achieve remote takeover of local instances

Adam Bannister 15 March 2021 at 13:55 UTC
Updated: 25 May 2021 at 15:08 UTC

Zero-day | Vulnerabilities | Cloud Security

Project maintainers reportedly declined to fix flaws due to limited attack scenarios

Critical vulnerabilities in LocalStack, a popular framework for building cloud applications, can be chained to remotely take over locally-run LocalStack instances, security researchers claim.

Researchers from Sonarsource have documented how they combined cross-site scripting (XSS) and server-side request forgery (SSRF) vulnerabilities to achieve OS command injection against the open source Python application.

However, the vulnerabilities remain unpatched in subsequently released LocalStack versions – v0.12.6 and v0.12.7 – after the project maintainers determined that real-world attack scenarios were "limited", Sonarsource researcher Dennis Brinkrolf said in a blog post published on March 2.

Attacking the Stack

Researchers observed that LocalStack lacked authentication, probably because the software is "run locally or in a Docker environment, as recommended by the vendor" and therefore not directly exposed to the internet, suggested Brinkrolf.

"However, it is a common fallacy that this type of application cannot be attacked" by external actors, he added, citing how so-called 'drive-by pharming attacks' have previously compromised network routers via their web interface.

Read more of the latest cloud security news

Citing a Sonarsource video demonstrating the LocalStack attack, Johannes Dahse, head of R&D at the Swiss infosec firm, told *The Daily Swig*: "All it takes is to host a malicious website, for example with interesting content related to LocalStack.

"If an attacker is motivated to target a LocalStack developer, we think that she/he will likely succeed."

LocalStack's project maintainers have yet to respond to questions emailed to them by *The Daily Swig*, but we will update the article should we receive a response.

CORS for concern

LocalStack is used to set up AWS cloud environments within local networks in order to develop and test cloud and serverless apps.

The researchers found that remote attackers could interact with locally-running LocalStack instances through the victim's browser, which they might use to read documentation, suggested Brinkrolf.

"When this victim visits (or is lured to) a malicious/infected website controlled by an attacker, it is possible to trigger cross-site HTTP requests to the victim's local network via JavaScript code."

Although this means "an attacker can send arbitrary requests from a website to a LocalStack instance", the cross-origin resource sharing (CORS) mechanism deployed by popular browsers blocks it from reading the responses, said the researcher.

Catch up on the latest security vulnerability news

However, sending the attack payload blindly can still be "sufficient to carry out a successful attack via" cross-site request forgery (CSRF) techniques.

Latest Posts

Deserialized web security roundup
Fortinet, Citrix bugs; another Uber breach; hacking NFTs at Black Hat

Critical IP spoofing bug patched in Cacti
'Not that hard to execute if attacker has access to a monitoring platform running Cacti'

Casting a SpEL
Akamai WAF bypassed via Spring Boot to trigger RCE

"Moreover, LocalStack explicitly allows the execution of cross-origin requests through any page by setting special HTTP headers in the response," continued Brinkrolf.

"This means that the attacker can detect and attack a LocalStack instance through the XHR response and does not actually operate blindly."

Although leading browsers have recently tightened CORS restrictions "to reduce the potential of CSRF attacks", these were bypassed by an XSS vulnerability uncovered by the researchers.

MitM backdoor

The CSRF payload can also reconfigure the edge router that relays requests to LocalStack APIs and add a proxy "that points to an attacker-controlled IP as proxy host", leading to a persistent SSRF vulnerability.

Because "the server copies the entire HTTP request from the client and forwards it to the server", the client's HTTP headers – including the AWS Cloud authorization header – are then "sent to the attacker-controlled server", paving the way to "session hijacking and stealing sensitive data from the test cloud".

And since the SSRF request's HTTP response "is printed unsanitized in LocalStack", an XSS payload from the attacker's server leads to a persistent manipulator-in-the-middle (MitM) proxy that "enables abuse of further features" and the potential "to trigger other code vulnerabilities" – including the command injection vulnerability outlined in Brinkrolf's blog post.

The researchers say they also uncovered a regular expression denial-of-service (ReDoS) bug in the platform.

Real-world threat?

Brinkrolf said Sonarsource first notified LocalStack maintainers of the vulnerabilities in October 2020 and contacted them on a further two occasions, before a response arrived in January indicating that the maintainers saw the application's local execution as a significant barrier to exploitation.

"While we agree that real-world attacks against local instances are less likely than against directly exposed applications, we believe that developers should be aware of these risks in order to protect their setups," said Brinkrolf.

Johannes Dahse added: "In order to keep the attack surface as small as possible we believe all code vulnerabilities should be addressed."

DON'T FORGET TO READ Git vulnerability could enable remote code execution attacks during clone process

Zero-day | Vulnerabilities | Cloud Security | Phishing | Social Engineering | MitM | Privacy | XSS | Research | Hacking Techniques | Hacking News | RCE | SSRF | CSRF | Browsers | Network Security | Open Source Software | Secure Development | Authentication | Industry News | JavaScript | Switzerland | Europe | Organizations | Enterprise | Python

Adam Bannister

@Ad_Nauseum74

Related stories

Deserialized web security roundup

Fortinet, Citrix bugs; another Uber breach; hacking NFTs at Black Hat

16 December 2022

Critical IP spoofing bug patched in Cacti

15 December 2022

Casting a SpEL

Akamai WAF bypassed via Spring Boot to trigger RCE

14 December 2022

Cloud flaws brought to the fore as bug bounty vulnerabilities hit 65k in 2022

13 December 2022