Oxeye Security Researchers Discover "ParseThru" - Parameter Smuggling Vulnerability in GoLang-based Applications

Security Gap Permits Threat Actors to Bypass Validations and Gain Unauthorized Access to Cloud Native Applications

Oxeye Logo

TEL AVIV, ISRAEL, August 2, 2022 /EINPresswire.com/ -- Oxeye, the provider of an award-winning cloud-native application security platform, today announced the discovery of “ParseThru” - a new vulnerability found in GoLang-based applications. GoLang is a popular cloud native programming language. It reduces the number of software development dependencies and has a short learning curve. Used to develop many cloud-native applications, GoLang is behind a large number of applications written for the cloud, including Kubernetes environments. The newly discovered vulnerability allows a threat actor to bypass validations under certain conditions, as a result of the use of unsafe URL parsing methods built in the language.

Every programming language has its own implementation of URL parsing logic. GoLang uses the ‘net/url’ library to parse URLs. Prior to version 1.17 of the programming language, GoLang would consider semicolons in the query part of the URL as a valid delimiter. However, after version 1.17, GoLang changed this behavior, and now the “parseQuery” method will return an error if the query part of the URL contains a semicolon. Although this method was fixed to properly return an error when the input contains a semicolon, one of the methods responsible for getting the parsed query string bluntly ignores the error returned.

As a result, when a GoLang-based public API built upon GoLang version greater than 1.17 communicates with an internal service running GoLang prior to v1.17. When a user makes an http request to the first service, supplying a query parameter, the service will make a determination on whether to pass on the request based on the supplied parameter. If a semicolon is added to the named parameter, the first service will ignore its existence. No logic will be made based on the actual parameter value. At this point, the request is forwarded to the internal service, receiving and treating the request the latter receives the transaction and treats the parameter without the semicolon. This means miscreants are able to smuggle requests

containing query parameters that would normally be rejected.

While conducting this research, Oxeye discovered multiple instances of this behavior in several open-source projects which resulted in various vulnerabilities. Three identified vulnerable projects include CNCF graduated project Harbor, an open source registry that secures artifacts with policies and role-based access control; Traefik, a modern http reverse proxy and load balancer that makes deploying microservices easy and Skipper, an http router and reverse proxy for service composition. For these and other open source projects, the Oxeye research team managed to bypass critical application logic using this vulnerability to exploit the application for performing various unauthorized actions.

“With our experts uncovering this security issue, we now recommend that GoLang-based apps in use should be reviewed to ensure the proper patching and/or remediation is applied,” said Ron Vider, CTO and Co-founder, Oxeye. “As noted above, the initial review by Gal Goldshtein and Daniel Abeles has revealed that several significant open source projects have been impacted by this edge case. To assist with remediation, we are providing deeper technical dive into these vulnerabilities that can be found on the Oxeye blog at https://www.oxeye.io/blog/golang-parameter-smuggling-attack.”

If interested in learning more about how Oxeye can assist with cloud native application security challenges, please visit https://www.oxeye.io/get-a-demo to register for a demonstration.

Resources:
- Follow Oxeye on Twitter at @OxeyeSecurity
- Join Oxeye on LinkedIn at https://www.linkedin.com/company/oxeyeio/
- Visit Oxeye online at http://www.oxeye.io

About Oxeye
Oxeye provides a cloud-native application security solution designed specifically for modern architectures. The company enables customers to quickly identify and resolve all application-layer risks as an integral part of the software development lifecycle by offering a seamless, comprehensive, and effective solution that ensures touchless assessment, focus on the exploitable risks, and actionable remediation guidance. Built for Dev and AppSec teams, Oxeye helps to shift security to the left while accelerating development cycles, reducing friction, and eliminating risks. To learn more, please visit www.oxeye.io.

- END -

Dean Agron
Oxeye
+972 (54) 456-2587
email us here
Visit us on social media:

Facebook
Twitter
LinkedIn

This press release can be viewed online at: https://www.einpresswire.com/article/584105226

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2022 Newsmatics Inc. All Right Reserved.