

Vulnerabilities find in Project [deroproject/derohe](https://github.com/deroproject/derohe)

- 1) Affecting com.google.protobuf:protobuf-java artifact, versions [,3.4.0)
https://github.com/deroproject/derohe/blob/main/vendor/github.com/prometheus/client_model/pom.xml

Overview

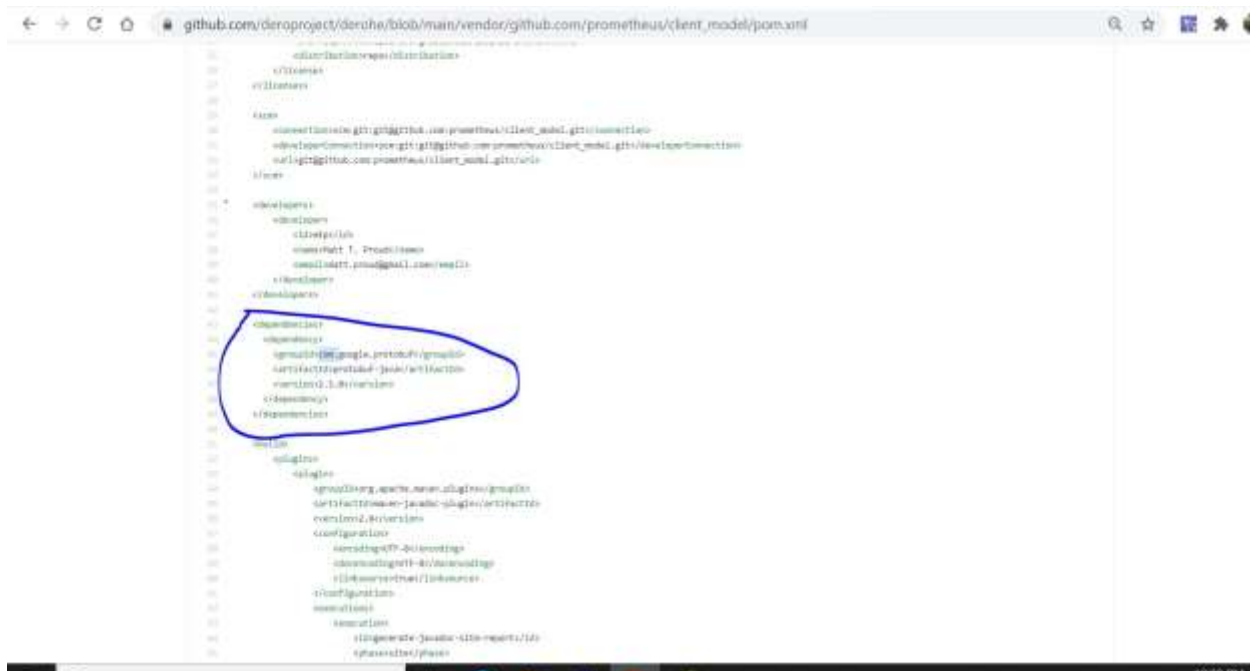
com.google.protobuf:protobuf-java is a Google's language-neutral, platform-neutral, extensible mechanism for serializing structured data. Affected versions of this package are vulnerable to Integer Overflow by allowing remote authenticated attackers to cause a heap-based buffer overflow in serialization process.

Remediation

Upgrade com.google.protobuf:protobuf-java to version 3.4.0 or higher.

Ref: <https://github.com/protocolbuffers/protobuf/issues/760>

Evidence



The screenshot shows a web browser displaying a GitHub repository page for the file `github.com/deroproject/derohe/blob/main/vendor/github.com/prometheus/client_model/pom.xml`. The XML content is visible, and a blue circle highlights the following dependency entry:

```
<dependency>  
  <groupId>com.google.protobuf</groupId>  
  <artifactId>protobuf-java</artifactId>  
  <version>3.4.0</version>  
</dependency>
```

- 2) golang.org/x/text Denial of Service (DoS)

Introduced through: github.com/ybbus/jsonrpc/v2@0.0.0 › github.com/onsi/gomega@v1.5.0 › golang.org/x/text@v0.3.0

<https://github.com/deroproject/derohe/blob/main/vendor/github.com/ybbus/jsonrpc/jsonrpc.go>

Overview

golang.org/x/text/encoding/unicode is an unicode package provides Unicode encodings such as UTF-16.

Affected versions of this package are vulnerable to Denial of Service (DoS). It is possible to exploit the UTF-16 decoder into entering an infinite loop, causing the program to crash or run out of memory.