

Remote session stealing of Hikvision Access Control/Intercom Products

Vulnerability description

Remote attacker can steal valid authentication session ID-s of Hikvision Access Control/Intercom Products. This is possible because a remote attacker can create a session ID-s without restrictions. If an attacker requests a session ID at the same time as a valid user, the attacker receives the identical session ID. This session ID is immediately recognized as valid after successful authentication of the correct user.

The authentication session key generation can be initiated in an API interface and requested without providing password. Therefore anyone can request session ID linked to any user.

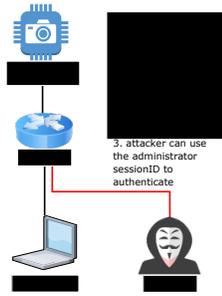
The session ID becomes valid after successful authentication by legitimate user with valid username and password. If an attacker and a legitimate user access the API at the same time,

they receive the same session key. If the user's authentication was successful, the session key becomes valid and can also be used by an attacker to authenticate with rights of the legitimate user.

The attack can be simply described by following steps:

1. Attacker initiates connection ISAPI to generate sessionID
2. The user authenticates and gets sessionID from ISAPI
3. If attacker and user requests key generation from ISAPI at same time, the same sessionID is being generated
4. The attacker uses same sessionID to authenticate
5. The attacker has authenticated access to management web portal and API

Attack topology:



Impact

- The attacker could open door from remote location
- The attacker could issue PIN to open door locally
- The attacker could access video/audio stream
- The attacker could change configuration, add users etc.

PoC scripts

ISAPI sessionID generation script:

Download: [request_ids.py](#)

```
usage example:  
python3 request_ids.py 192.168.1.11
```

Valid session request script:

Download: [validate.sh](#)

```
to generate an authentication cookie this script also request nonce  
from API which is static value for device  
usage example:  
validate.sh hik-sessions_192.168.1.11--12-01-2023--01_00_45.txt  
192.168.1.11
```

PoC video:



0:00 / 1:50

Download PoC video: [video.mp4](#)

Details of the vulnerability	
CVE number	CVE-2023-28809
Weakness ID	CWE-304: Missing Critical Step in Authentication
CVSS 3.1	AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CVSS Base Score	8.8 (High)
Date	12.01.2023
Affected products and versions	
DS-K1T804AXX Fingerprint Terminals	Versions below V1.4.0_build221212 (including V1.4.0_build221212)
DS-K1T341AXX Face Recognition Terminals	Versions below V3.2.30_build221223 (including V3.2.30_build221223)
DS-K1T671XXX Face Recognition Terminals	Versions below V3.2.30_build221223 (including V3.2.30_build221223)
DS-K1T343XXX Face Access Terminals	Versions below V3.14.0_build230117 (including V3.14.0_build230117)
DS-K1T341C Face Recognition Terminals	Versions below V3.3.8_build230112 (including V3.3.8_build230112)
DS-K1T320XXX Face Access Terminals	Versions below V3.5.0_build220706 (including V3.5.0_build220706)

To Top

[← Back](#)

hinnoaar.com