![Dahua Technology logo]

# Security Advisory – Unauthorized Device Timestamp Modification Vulnerability Exists in Some Dahua Embedded Products

**Advisory ID**：DHCC-SA-202302-001

**First Published**：2023-02-08

## Summary

Some Dahua embedded products have a vulnerability of unauthorized modification of the device timestamp. By sending a specially crafted packet to the vulnerable interface, an attacker can modify the device system time.

## CVE ID

CVE-2022-30564

## Vulnerability Score

The vulnerability classification has been performed by using the CVSSv3.1 scoring system (http://www.first.org/cvss/specification-document).

CVE-2022-30564
Base Score：5.3（AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N）
Temporal Score：4.6（E:U/RL:O/RC:C）

## Affected Products & Fix Software

The following product series and models are currently known to be affected.

| Product Series | DNA Model |
|---|---|
| IPC | N45EF63, N45EJ62, N45EM63, N45EFN2, N45EJN2, N45EYN2, N45EFNZ, N45EYNZ, N85EFN2 |
| | DH-IPC-HDBW5442HN-ZHE, N45DB7Z, N45DJ62, N45DL7Z, N45DM62, DH-IPC-HDBW5842EN-Z4E-S2, DH-IPC-HFW5842EN-Z4E-S2, N85DB6Z, N85DF62, N85DJ62, N85DJ6Z, N85DL6Z, N85DY62 |
| | N55DU82, N55DY82 |
| | N43BX82, N43BU82, N43BU83, N83BU82 |
| PTZ | 49425XBNR, 50232XANR, 50432XANR, 52C232XANR, 52C432XANR, 59232XANR, 5A445XANR, 6AL445XANR, 6CE445XANR, 1A404XBNR |
| | 22204UENI, 22204UENI-W |
| | 6C3425XBPV |

| NVR | DHI-NVR5216-16P-I |
| --- | --- |
| | DH-NVR4216-16P-I |
| XVR | X82R2A Gen 1 Chipset, X82B3A Gen 1 Chipset, X82B2A Gen 1 Chipset, X51C1E Gen 1 Chipset, X51C2E Gen 1 Chipset, X81B1E Gen 1 Chipset, X51C3E Gen 1 Chipset, X52B3A Gen 1 Chipset, X54B5L Gen 1 Chipset, X88B5S Gen 1 Chipset, X84R3L Gen 1 Chipset, X82R3N Gen 1 Chipset |
| | X72A2A, X72A3A, X74A3L, X72B2A, X51A1E, X51A2E, X51A3E, X52A3A, X52A3N, X54A5L, X58A5S |
| | X82A3A |

Note: Please login to the Web interface of the device to view Build time, which you can find on the Settings-System Information-Version Information page (setting-systeminfo-version).

## Fix Software Download

Please download the corresponding fix software or its newer version as listed in the above table from Dahua website, or contact Dahua local technical support to upgrade.

- Cloud Upgrade：For products with cloud upgrade capability, the related repair version will be successively pushed through the cloud upgrade within 30 working days.
- Dahua Wiki: https://dahuawiki.com/Main_Page
- Dahua Technical Support Personnel.

## Support Resources

For any questions or concerns related to our products and solutions, please contact Dahua DHCC at cybersecurity@dahuatech.com.

## Acknowledgment

We acknowledge the support of Souvik Kandar and Arko Dhar from Redinent Innovations, India who discovered this vulnerability, and we also want to acknowledge the cooperation of the National Computer Emergency Response Team of India (CERT-In) who reported it to DHCC and coordinated with us to handle this vulnerability.

## Revision History

| Version | Description | Date |
| --- | --- | --- |
| V1.0 | Initial public release | 2023-02-08 |