Dahua Technology USA Inc.
23 Hubble, Irvine, CA 92618 | us.dahuasecurity.com
Office 949.679.7777 | Fax 949.679.5760

SECURITY ADVISORY

Session ID Predictable Vulnerability Found in Some Dahua Products
2020-5-11

SA ID：DHCC-SA-202005-003

First Published：2020-5-11

Summary:

1. **CVE-2020-9502**：**Session ID Can Be Predicted Vulnerability**

Some Dahua products have Session ID predictable vulnerabilities. During normal user access, an attacker can use the predicted Session ID to construct a data packet to attack the device.

Vulnerability Score (CVSS V3.1 http://www.first.org/cvss/specification-document):

CVE-2020-9502

Base Score：8.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Temporal Score：7.9 E:P/RL:O/RC:C

Affected Products:

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

Product Line	Product Series	Time
SD	6AL Series	~2019.12
	5A Series	
	1A Series	
	50/52C Series	
NVR	NVR N5x Series	~2019.12
	NVR N4x Series	
IPC	N4 Series	

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).

Dahua Technology USA Inc.
23 Hubble, Irvine, CA 92618 | us.dahuasecurity.com
Office 949.679.7777 | Fax 949.679.5760

Fix Software Download:

Please download the corresponding fix software or its newer version that addresses above vulnerabilities from Dahua Wikipedia: https://dahuawiki.com/Firmware_Update/April_2020_Firmware_Update or contact Dahua technical support.

Support Resources:

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

We acknowledge the support of Thomas Vogt from the University of Applied Sciences Offenburg who discovered this vulnerability and reported to DHCC.