

SECURITY ADVISORY

Login Authentication Compatibility Vulnerabilities Found in Some Dahua Products
2020-5-11

SA ID : DHCC-SA-202005-002

First Published : 2020-5-11

Summary:

1. CVE-2019-9682 : Login Authentication Compatibility Vulnerability

Dahua devices use strong security login mode by default, but in order to be compatible with the normal login of early devices, some devices retain the weak security login mode that users can control. If the user uses a weak security login method, an attacker can monitor the device network to intercept network packets to attack the device. So it is recommended that the user disable this login method.

Vulnerability Score (CVSS V3.0) <http://www.first.org/cvss/specification-document>):

CVE-2020-9682

Base Score : 8.1 CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Temporal Score : 7.3 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).



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 Bashis who discovered this vulnerability and reported to DHCC.