

PRODUCT BULLETIN

Date	21/12/2021		
Part Number	Hikvision - Various		
Description	Apache Log4j Remote Code Execution Vulnerability		
ITEM 1	<p>ADVISORY</p> <p>Most Hikvision hardware and software products are not affected by the LOG4J ZERODAY vulnerability.</p>		
DETAIL	HARDWARE PRODUCTS	AFFECTED?	VERSION
	Front-end(camera, PTZ, etc)	NO	
	Back-end(DVR, NVR, etc)	NO	
	transmission/display	NO	
	access control	NO	
	Alarm	NO	
	Intercom	NO	
	CVR	NO	
	SOFTWARE PRODUCTS	AFFECTED?	VERSION
	iVMS4200	NO	
	Hik-Connect	NO	
	3000N	NO	
	Hik-Central Pro	NO	
	Hik-Central Enterprise	NO	
iVMS5200M, iVMS5200P iVMS5200E	YES	ALL	
Hik-Central Master	YES	Hikcentral Master V1.0.0 Hikcentral Master liteV1.0.X, V.1.1.X V1.2.0	
REMEDY	<p>For iVMS5200 products, download and apply the instructions and patch from this location</p> <p>https://www.dropbox.com/s/zecw58xx89p1m7r/log4jUpdate fixing patch.zip?dl=0</p>		

www.ness.com.au

Ness Corporation Pty Ltd ABN 28 069 984 372 Private Bag 23 Seven Hills NSW 1730 Australia Ph +61 2 8825 9222 Fax +61 2 9838 8508 Email: ness@ness.com.au



Sydney
4 / 167 Prospect Hwy
Seven Hills NSW 2147
Phone 02 8825 9222
Fax 02 9674 2520
sales@ness.com.au

Melbourne
4 / 56 Norcal Rd
Nunawading VIC 3131
Phone 03 9875 6400
nessmelb@ness.com.au

Brisbane
Unit 5 / 16 Metroplex Ave
Murarrie QLD 4172
Phone 07 3399 4910
nessbris@ness.com.au

Adelaide
Unit 1 / 22 Ware St
Thebarton SA 5031
Phone 08 8152 0000
adelaide@ness.com.au

Perth
1 / 9 Inverness St
Malaga WA 6090
Phone 08 9328 2511
nessper@ness.com.au

Update for Apache Log4j2 Issue (CVE-2021-44228)

December 16, 2021

Dear valued partners,

Hikvision is actively following the recently disclosed security vulnerability in the open-source Apache "Log4j2" utility ([CVE-2021-44228](#)) that has been classified as "Critical" with a CVSS score of 10 and allows for Remote Code Execution with system-level privileges or sensitive information leak.

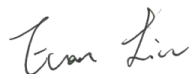
In addition to monitoring the threat landscape for attacks and developing customer protections, our security teams immediately launched an investigation upon learning of the vulnerability. Up to now, Hikvision has observed no indicators of compromise on our products from Log4j2. We would like to update you with the specific analysis results so far in below:

1. Hikvision's IPC, NVR, CVR, transmission and display products, access control products and alarm products are not affected by this vulnerability.
2. HikCentral Professional, HikCentral Enterprise, Hik-Connect, Hik-ProConnect, iVMS-4200 and iVMS-3000N are not affected by this vulnerability.

Hikvision will continue to actively monitor the development of this issue as it evolves and provide updates to you. Countermeasures are in place to provide layers of protection and increase situational awareness.

If you have further questions, please do not hesitate to contact us.

Kina regards,

A handwritten signature in black ink that reads "Evan Liu".

Evan Liu

Managing Director

Hikvision Oceania

Hikvision Oceania

Headquarter: U14A, 2 Eden Park Drive, Macquarie Park, NSW 2113, Australia

Main: +61 1300 557 450 / +64 (0) 92173127

Tech Support Line: +61 1300 976 305

Sales Email: sales.au@hikvision.com / sales.nz@hikvision.com

Website: www.hikvision.com