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

December 14, 2021

Dear valued partners:

Hikvison is aware of the recently disclosed security issue relating to the open-source Apache "Log4j2" utility (CVE-2021-44228) that has been classified as "Critical" with a CVSS score of 10, allowing 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 have immediately commenced the investigation and analysis once we received the information. 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 as 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 and iVMS-4200 are not affected by this vulnerability.

Hikvision will continue to actively monitor the development of this issue as it evolves and provide you the update if any. 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 via your Hikvision account manager in the first instance who will facilitate a further response.