

Update für Apache Log4j2 Problem (CVE-2021-44228)

14. Dezember 2021

Sehr geehrte Partner,

Hikvision ist sich der kürzlich bekannt gewordenen Sicherheitslücke im Zusammenhang mit dem Open-Source-Dienstprogramm Apache "Log4j2" (CVE-2021-44228) bewusst, die als "kritisch" mit einem CVSS-Score von 10 eingestuft wurde und die Remote Code Execution mit Privilegien auf Systemebene oder den Verlust sensibler Informationen ermöglicht.

Neben der Überwachung der Bedrohungslandschaft auf Angriffe und der Entwicklung von Kundenschutzmaßnahmen haben unsere Sicherheitsteams sofort nach Erhalt der Informationen mit der Untersuchung und Analyse begonnen. Bis jetzt hat Hikvision keine Anzeichen für einen Angriff auf unsere Produkte durch Log4j2 festgestellt. Im Folgenden möchten wir Sie über die bisherigen Analyseergebnisse informieren:

1. Die IPC-, NVR-, CVR-, Übertragungs- und Anzeigeprodukte, Zugangskontroll- und Alarmprodukte von Hikvision sind von dieser Sicherheitslücke nicht betroffen.
2. HikCentral Professional, HikCentral Enterprise, Hik-Connect, Hik-ProConnect und iVMS-4200 sind von dieser Sicherheitslücke nicht betroffen.

Hikvision wird die Entwicklung dieses Problems weiterhin aktiv verfolgen und Sie gegebenenfalls mit einem Update versorgen. Es wurden Gegenmaßnahmen ergriffen, um einen mehrschichtigen Schutz zu gewährleisten und das Situationsbewusstsein zu erhöhen.

Sollten Sie weitere Fragen haben, zögern Sie bitte nicht, uns zu kontaktieren.

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

December 14, 2021

Dear valued partners:

Hikvision 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 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 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 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.