Security Notice – Information on Apache Log4j2 Remote Code Execution Vulnerability CVE-2021-44228

First Publish Date: December 13, 2021

Summary

Dahua has noticed the disclosure of technical details and PoC for critical vulnerability of Apache Log4j2, CVE-2021-44228 recently, with Base CVSS Score: 10.0 (CVSS:3.0/AV:N/AC:L/PR:N/ UI:N/S:C/C:H/I:H/A:H). Attackers can directly construct malicious requests to exploit this vulnerability to trigger remote code execution.

Dahua immediately initiated technical analysis and product screening, and the preliminary investigation result is:

- Dahua Device products (including but not limited to: IPC, HDCVI, PTZ, ITC, NVR, DVR, Storage, Video Intercoms, Access Control & Time Attendance, Alarms, Interactive WhiteBoards, Video Conferencing, IVS, Security Screening, etc.) do not contain Apache Log4j2 components, so they are not affected by this vulnerability.
- Dahua Security Software(DSS) products（including: DSS Express v8.0, DSS Pro v7.002/v8.0, DSS4004-S2 v8.0, DSS7016D-S2 v8.0）contain Apache Log4j2 components, so these products were affected by this vulnerability.

  As for latest update, Log4j version is expected to be released soon, we are currently evaluating the impact and closely monitoring the development. We will keep you informed if any necessary update is required.

We will keep you updated in our "security advisories" page if any necessary update is required.

URL:
https://www.dahuasecurity.com/support/cybersecurity/annoucementNotice

Support Resources

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

Zhejiang Dahua Technology Co., Ltd

2021-12-13