BOSCH

Security Information

Apache Log4j Vulnerability (CVE-2021-44228) "Log4Shell"
(https://nvd.nist.gov/vuln/detail/CVE-2021-44228)

We are aware of the Apache Log4j Vulnerability (CVE-2021-44228) "Log4Shell".

We are currently analyzing if any of our products are affected. In case any of our products are affected, we will publish respective Security Advisories on this web site:
https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html.

Remote Portal and Cloud Analytics Services are all patched to a non-vulnerable version of Log4j and were not impacted.

Our analysis so far (see timestamp at end of this document) showed the following products **ARE NOT AFFECTED:**
(the following list will be updated as new information is available)

BT-VS
• IP Cameras (all families CPP4-14)
• VIDEOJET decoder (VJD-7513, VJD-8000)
• Video Recording Manager (VRM)
• Configuration Manager
• Monitor Wall
• Project Assistant
• Video Security App (Android & iOS)
• Video Security Client
• Tracking & Recognition Service (TRS)
• VideoSDK
• BVMS
• Intelligent Insights
• DIVAR hybrid/network
• DL 380 Servers
• E2800 Storage Arrays

BT-CO
• Intercom products

BT-AI/PAA
• AEC – Access Easy Controller
• AEMC
• AMS – Access Management System
• AMC2 – Access Modular Controller
• APE – Access Professional Edition
• BIS ACE – Building Integration System, Access Control Engine
• SE – Security Escort

BT-AI/PAI
• Sensors
• Nothing on panel/system side is Java based
• B Series and G Series systems products, including the G450
• Installer Service Portal patched to a non-vulnerable version of Log4j and was not impacted.

BT-FIR
• Panels:
  − FPA-1200/5000 controller
  − AVENAR controller
  − FPC-500 controller
• Applications:
  − FPA-5000 OPC Server
• Remote Services:
  − Secure Network Gateway
  − Remote Connect (patched; see Remote Portal)
  − Remote Maintenance (patched; see Remote Portal)
  − Remote Alert (patched; see Remote Portal)

BT-IE
• UGM2040
• FASOS
• Energy Platform