LEGRAND – DPC
SECURITY INFORMATION

Dominion® KX IV – 101 v4.5

Dawn Syskowski – Updated 08/042025

TABLE OF CONTENTS

Device Operating System - Security | DKX4-101 Firmware v4.5

- At Legrand, there is a heightened awareness of the impact that poor product security could have on the end customer.
- As part of our Xerus firmware development cycle and ongoing threat assessment, Legrand runs a security scanner on KX4-101 firmware releases. Legrand owns a Nessus Vulnerability scanner license which gets renewed every year. Before a new KX4-101 firmware gets released we test it with this scanner tool. As soon as a new Nessus scanner version is available from the vendor, Tenable, Legrand will update the scanner tool to it‘s latest version.
- KX4 firmware supports FIPS 140-2 mode configuration
- During a firmware release system test cycle, security-related firmware features are tested.
- KX4 firmware requires an immediate change from the default user password to a new password
- KX4 firmware requires strong passwords to be created as the default behavior
- Legrand has a Security Working Group which is dedicated on staying ahead of the requirements for security.

Operating System – Security Stack

DKX4-101 Firmware v4.5

- The Operating System source code is solely based on:
  - Source Code written and owned by Raritan (proprietary source code) and
  - Open Source library and program source code (a complete list of all used Open Source libraries can be provided on demand)
- The SSH stack is based on:
  - Package: Dropbear
  - Version: 2024.85
  - URL : http://matt.ucc.asn.au/dropbear/dropbear.html
  - License: MIT
- The SSL stack is based on:
  - Package: openssl
  - Version: 3.0.14
  - FIPS Version: 3.0.9
  - URL : http://www.openssl.org/
  - License: OpenSSL
  - Note: own license (http://www.openssl.org/source/license.html)

Operating System – Security | DKX4-101 Firmware v4.5

- Details about the encryption technology, • cryptographic libraries • algorithms • mode choices:
  - OpenSSL
    - TLS 1.0, 1.1. disabled
    - TLS 1.2 and 1.3 enabled by default
    - Supported TLS cipher- and mode combinations in order of priority (priority is server enforced):
      - TLS 1.2:
        - TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
        - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
        - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
      - TLS 1.3:
        - TLS_AKE_WITH_CHACHA20_POLY1305_SHA256
        - TLS_AKE_WITH_AES_128_GCM_SHA256
        - TLS_AKE_WITH_AES_256_GCM_SHA384
  - Unused protocols like SSL2, SSL3, DTLS, SRP and unused algorithms are not compiled in to reduce attack risk
  - Upstream code is monitored by engineering for updates and decided on case-by-case when to integrate it in the firmware. I.e. depending on if the product is affected and the severity of an issue it is determined if an intermediate update is provided or if the changes are available with the next regular release.

Operating System – Security

DKX4-101 Firmware v4.5

- Dropbear SSH Server:
  - Key Exchange
    - curve25519-sha256@libssh.org
    - curve25519-sha256
    - ecdh-sha2-nistp521
    - ecdh-sha2-nistp384
    - ecdh-sha2-nistp256
    - kexguess2@matt.ucc.asn.au
    - Kex-strict-s-v00@openssh.com
  - Host Key Algorithms:
    - ecdsa-sha2-nistp384
    - ssh-ed25519
    - rsa-sha2-256

Operating System – Security | DKX4-101 Firmware v4.5

- Ciphers:
  - aes128-ctr
  - aes256-ctr
  - chachat20-poly1305@openssh.com
- MACs:
  - hmac-sha2-256
  - hmac-sha2-512

- TLS:
  - customer can create/upload custom certificates
  - client code does certificate and hostname verification (i.e. rejects invalid certificates)
- SNMPv3:
  - AES and DES
- User credentials (passwords) are hashed using PBKDF2 function (SHA256, 3000 rounds, 12 bytes salt)
- HTTP access is re-directed to HTTPS.
- Default password policy requires user to set a new password prior to operation in a production environment
- 802.1x:
  - 802.1x can be configured for physical ethernet router security and validation.
- IP Access control can be enabled to allow/disallow device access from IP ranges
- Strong passwords enabled by default, password strength requirements can be configured
- Disable user accounts because of failed login attempts