Vulnerabilities in dormakaba products

Installations of Kaba exos 9300 systems, before version 4.4.0, are affected by vulnerabilities. Especially if a system is not hardened according to our Security Guidelines, it is possible to gain access to the Kaba exos 9300 database and derive sensitive Information, take control of Access Managers or escalate the privileges of a local user on the Kaba exos 9300 Application Server.

To exploit these vulnerabilities, an attacker would need prior access to the network or the hardware. Exploitation is only possible from within the internal network.

Advisory Information

ID:	DKSA-26-26-012	
CVE Numbers and Scores:	CVE-2025-59090	9.3 (Critical)
	CVE-2025-59091	9.3 (Critical)
	CVE-2025-59092	8.7 (High)
	CVE-2025-59093	8.5 (High)
	CVE-2025-59094	7.0 (Medium)
	CVE-2025-59095	6.8 (Medium)
	CVE-2025-59096	4.6 (Medium)
Published:	26 January 2026	
Advisory Version:	1	

Affected Products

- Kaba exos 9300
  - All Versions

Mitigations

Update to latest release, at least exos 9300 version 4.4.1, and perform mitigation tasks to secure the communication and harden the overall system.

It is highly recommended to encrypt the communication to the Access Manager 92xx K5 “exos Client” via IPSec and to the Access Manager 92xx K7 “exos Client” via mTLS (https).

Details and further information on mitigation measures can be found under Vulnerability Details.

Recommendation

	Risk	Recommendation
✓	**High/Critical**	Updates should be applied as soon as possible based on organizational needs and threat model.
	Medium	Within six months, based on organizational needs and threat model
	Low	During the next scheduled update cycle or within a year
	None / Info	Based on organizational needs and after appropriate testing

Vulnerability Details

CVE-2025-59090 Unauthenticated SOAP API

On the Kaba exos 9300 server, a SOAP API is reachable on port 8002. This API does not require any authentication prior to sending requests. Therefore, network access to the exos server allows e.g. the creation of arbitrary access log events as well as querying the 2FA PINs associated with the enrolled chip cards.

- Classification / Type
  - CWE-306: Missing Authentication for Critical Function
  - CWE-1188: Initialization of a Resource with an Insecure Default
- CVSS Vector:
  - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N
- Base Score: 9.3 (Critical)
- Estimated Risk: Critical
- Affected Versions: All Versions older than 4.4.0

- Mitigation Details:
  - It is highly recommended to encrypt the communication to the Access Manager 92xx K5 via IPSec. The Configuration is described in the device reference manual. It is also recommended to secure the used communication port from external access.
  - To encrypt the communication to the Access Manager 92xx K7, an mTLS connection can be set up. For new installations in combination with exos 4.4.x, HTTPS with self-signed certificates is activated by default. In existing installations, this must be configured manually. HTTPS with self-signed certificates can be configured at any time. The configuration is described in the device reference manual. It is also recommended to secure or close the used communication port from external access.

CVE-2025-59091 Hardcoded Legacy Accounts Allowing Control Over Access Managers

Multiple hardcoded credentials have been identified, which are allowed to sign-in to the Kaba exos 9300 datapoint server running on port 1004 and 1005. This server is used for relaying status information from and to the Access Managers. This information, among other things, is used to graphically visualize open doors and alerts. However, controlling the Access Managers via this interface is also possible.

To send and receive status information, authentication is necessary. The Kaba exos 9300 application contains hard-coded credentials for four different users, which are allowed to login to the datapoint server and receive as well as send information, including commands to open arbitrary doors.

- Classification / Type
  - CWE-798: Use of Hard-coded Credentials
- CVSS Vector:
  - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N
- Base Score: 9.3 (Critical)
- Estimated Risk: Medium
- Affected Versions: All Versions older than 4.4.1
- Mitigation Details:
  - An update to the latest exos version is recommended, at least exos 4.4.1. The connections to the datapoint server are not protected by default. We recommend protecting the port 1005 accordingly with external means (e.g. IPsec).

CVE-2025-59092 Unauthenticated RPC Service

An RPC service, which is part of Kaba exos 9300, is reachable on port 4000, run by the process FSMobilePhoneInterface.exe. This service is used for interprocess communication between services and the Kaba exos 9300 GUI, containing status information about the Access Managers. Interacting with the service does not require any authentication. Therefore, it is possible to send arbitrary status information about door contacts etc. without prior authentication.

- Classification / Type
    - CWE-306: Missing Authentication for Critical Function
- CVSS Vector:
    - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N
- Base Score: 8.7 (High)
- Estimated Risk: Medium
- Affected Versions: All Versions older than 4.4.0, depending on Configuration
- Mitigation Details:
    - An update to the latest exos version is recommended, at least exos 4.4.0.

CVE-2025-59093 Insecure Password Derivation Function for Database Administrator

Exos 9300 instances are using a randomly generated database password to connect to the configured MSSQL server. The password is derived from static random values, which are concatenated to the hostname and a random string that can be read by every user from the registry. This allows an attacker to derive the database password and get authenticated access to the central exos 9300 database as the user Exos9300Common. The user has the roles ExosDialog and ExosDialogDotNet assigned, which are able to read most tables of the database as well as update and insert into many tables.

- Classification / Type
    - CWE-656: Reliance on Security Through Obscurity
- CVSS Vector:
    - CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
- Base Score: 8.5 (High)
- Estimated Risk: Medium
- Affected Versions: All Versions, depending on Configuration

- Mitigation Details:
  - As mitigation, direct access to the database and manipulation of the rich client or their communication must be ruled out. This can be achieved by operating the rich clients and their application services in a secure environment with a correspondingly limited connection to the user.

CVE-2025-59094 Local Privilege Escalation in exos 9300 System management

A local privilege escalation vulnerability has been identified in the Kaba exos 9300 System management application (d9sysdef.exe). Within this application it is possible to specify an arbitrary executable as well as the weekday and start time, when the specified executable should be run with SYSTEM privileges.

- Classification / Type
  - CWE-269: Improper Privilege Management
- CVSS Vector:
  - CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
- Base Score: 8.4 (High)
- Estimated Risk: Medium
- Affected Versions: All Versions
- Mitigation Details:
  - Rich clients are vulnerable to insider attacks. If there is a need for protection (against insiders or people with access to the network), the rich clients must operate in a protected environment. Alternatively, the web client is suitable for most use cases.

CVE-2025-59095 Hard-coded Key for PIN Encryption

The program libraries (DLL) and binaries used by exos 9300 contain multiple hard-coded secrets. One notable example is the function "EncryptAndDecrypt" in the library Kaba.EXOS.common.dll. This algorithm uses a simple XOR encryption technique combined with a cryptographic key (cryptoKey) to transform each character of the input string. However, it's important to note that this implementation does not provide strong encryption and should not be considered secure for sensitive data. It's more of a custom encryption approach rather than a common algorithm used in cryptographic applications. The key itself is static and based on the founder's name of the company. The functionality is for example used to encrypt the user PINs before storing them in the MSSQL database.

- Classification / Type
  - CWE-798: Use of Hard-coded Credentials

- CVSS Vector:
  - CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N
- Base Score: 6.8 (Medium)
- Estimated Risk: Medium
- Affected Versions: All Versions older than 4.3.3
- Mitigation Details:
  - An update to the latest exos version is recommended, at least exos 4.3.3.

CVE-2025-59096 Weak Default Password

The default password for the extended admin user mode in the application U9ExosAdmin.exe ("Kaba 9300 Administration") is hard-coded in multiple locations as well as documented in the locally stored user documentation.

- Classification / Type
  - CWE-798: Use of Hard-coded Credentials
- CVSS Vector:
  - CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N
- Base Score: 4.6 (Medium)
- Estimated Risk: Low
- Affected Versions: All Versions, depending on Configuration
- Mitigation Details:
  - Make sure to change the default password for the extended admin mode in the admin tool to a new password.

Additional Information

Legal Disclaimer

Please ensure that your security measures comply with relevant regulatory requirements in the multifamily housing industry, including privacy and notification obligations.

Terms of Use

Additional Resources

- https://dormakabagroup.com/en/security
- securitysupport@dormakaba.com
- https://sec-consult.com/de/vulnerability-lab/

Appendix

Acknowledgements

dormakaba thanks Werner Schober and Clemens Stockenreitner for their responsible disclosure of this issue, which enabled the development of mitigation measures prior to public disclosure, as well as for their commendable collaboration throughout the process.

CVSS Scoring

Vulnerability classification has been performed using the CVSS v4.0 scoring system. The base score should be supplemented with an analysis of the affected environment (i.e., Environmental Metrics).

The CVSS scores defined in this advisory are intended to measure the severity of specific vulnerabilities and should not be used alone to assess risk.

Severity	A qualitative measure of a vulnerability within the scope of a specific system.
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence (NIST SP 800-30).

Estimated Risk Scores

dormakaba qualifies identified vulnerabilities using the OWASP Risk Rating Matrix, assessing likelihood and impact to ensure a consistent, transparent, and business-relevant severity classification based on the system's standard configuration and a "typical" user's environment. This approach supports dormakaba's responsible disclosure process by communicating an estimated risk and remediation prioritization to stakeholders.