Vulnerabilities in dormakaba products

The dormakaba 9200, 9230 and 9290 Generation K5 and K7 with Firmware “exos Client”, Type Access Manager in older Versions are affected by vulnerabilities. Especially if a system is not hardened according to our Security Guidelines, it is possible to gain access to sensitive Information.

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-26-26-011	
CVE Numbers and Scores:	CVE-2025-59097	9.3 (Critical)
	CVE-2025-59098	8.7 (High)
	CVE-2025-59099	8.8 (High)
	CVE-2025-59100	5.9 (Medium)
	CVE-2025-59101	7.7 (High)
	CVE-2025-59102	6.9 (Medium)
	CVE-2025-59103	9.2 (Critical)
	CVE-2025-59104	7.0 (High)
	CVE-2025-59105	7.0 (High)
	CVE-2025-59106	- (Low)
	CVE-2025-59107	8.5 (High)
	CVE-2025-59108	9.2 (Critical)
Published:	26 January 2026	
Advisory Version:	1	

Affected Products

- Dormakaba Access Manager
    - Firmware "exos Client", Type Access Manager
    - Generation "K5" & "K7"

Mitigations

Access Manager 92xx-K5 exos Client:

- Update to XAMB 04.06.212 RA or later
- Encrypt the communication to exos 9300 via IPSec

Access Manager 92xx-K7 exos Client:

- Update to BAME 06.00 RA or later
- Encrypt the communication to exos 9300 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-2025-59097 Unauthenticated SOAP API

The exos 9300 application can be used to configure Access Managers (e.g. 9200, 9230 and 9290). The configuration is done in a graphical user interface on the dormakaba exos server. As soon as the save button is clicked in exos 9300, the whole configuration is sent to the selected Access Manager via SOAP. The SOAP request is sent without any prior authentication or authorization by default. Though authentication and authorization can be configured using IPsec for 9200-K5 devices and mTLS for 9200-K7 devices, it is not enabled by default and must therefore be activated with additional steps.

This insecure default allows an attacker with network level access to completely control the whole environment. An attacker is for example easily able to conduct the following tasks without prior authentication:

- Re-configure Access Managers (e.g. remove alarming system requirements)
- Freely re-configure the inputs and outputs - Open all connected doors permanently
- Open all doors for a defined time interval
- Change the admin password
- and many more

Network level access can be gained due to an insufficient network segmentation as well as missing LAN firewalls. Devices with an insecure configuration have been identified to be directly exposed to the internet.

- 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:H/SC:N/SI:N/SA:N
- Base Score: 9.3 (Critical)
- Estimated Risk: Critical
- Affected Versions:
  - 92xx-K5: All Versions
  - 92xx-K7: All Versions older than BAME 06.00 RA
- Mitigation Details:
  - 92xx-K5:

    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.

- 92xx-K7:

  To encrypt the communication to the Access Manager 92xx K7, an mTLS connection can be set up. A firmware update to at least BAME 06.00 RA is recommended. 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-2025-59098 Trace Functionality Leaking Sensitive Data

The Access Manager is offering a trace functionality to debug errors and issues with the device. The trace functionality is implemented as a simple TCP socket. A tool called TraceClient.exe, provided by dormakaba via the Access Manager web interface, is used to connect to the socket and receive debug information. The data is permanently broadcasted on the TCP socket. The socket can be accessed without any authentication or encryption.

The transmitted data is based on the set verbosity level. The verbosity level can be set using the http(s) endpoint with the service interface password or with the guessable identifier of the device via the SOAP interface.

The transmitted data contains sensitive data like the Card ID as well as all button presses on Registration units. This allows an attacker with network level access to retrieve all entered PINs on a registration unit.

- Classification / Type
  - CWE-497: Exposure of Sensitive System Information to an Unauthorized Control Sphere
- CVSS Vector:
  - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N
- Base Score: 8.7 (High)
- Estimated Risk: High
- Affected Versions:
  - 92xx-K5: All Versions older than XAMB 04.06.212 RA
  - 92xx-K7: All Versions older than BAME 05.02.156 RA
- Mitigation Details:
  - 92xx-K5:

    To secure the Access Manager 92xx, it is highly recommended to update to the latest FW, at least XAMB 04.06.212 RA.
  - 92xx-K7:

    To secure the Access Manager 92xx, it is highly recommended to update to the latest FW, at least BAME 05.02.156 RA.

CVE-2025-59099 Unauthenticated Path Traversal

The Access Manager is using the open-source web server CompactWebServer written in C#. This web server is affected by a path traversal vulnerability, which allows an attacker to directly access files via simple GET requests without prior authentication.

Hence, it is possible to retrieve all files stored on the file system, including the SQLite database Database.sq3, containing badge information and the corresponding PIN codes. Additionally, when trying to access certain files, the web server crashes and becomes unreachable for about 60 seconds. This can be abused to continuously send the request and cause denial of service.

- Classification / Type
  - CWE-35: Path Traversal
- CVSS Vector:
  - CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:L/SC:N/SI:N/SA:N
- Base Score: 8.8 (High)
- Estimated Risk: High
- Affected Versions:
  - 92xx-K5: All Versions older than XAMB 04.05.21 RA
  - 92xx-K7: All Versions older than BAME 04.05.16 RA
- Mitigation Details:
  - 92xx-K5:

    To secure the Access Manager 92xx, it is highly recommended to update to the latest FW, at least XAMB 04.05.21 RA.
  - 92xx-K7:

    To secure the Access Manager 92xx, it is highly recommended to update to the latest FW, at least BAME 04.05.16 RA.

CVE-2025-59100 Unauthenticated Access to the SQLite Database

The web interface offers a functionality to export the internal SQLite database. After executing the database export, an automatic download is started and the device reboots. After rebooting, the exported database is deleted and cannot be accessed anymore. However, it was noticed that sometimes the device does not reboot and therefore the exported database is not deleted, or the device reboots and the export is not deleted for unknown reasons. The path where the database export is located can be accessed without prior authentication. This leads to the fact that an attacker might be able to get access to the exported database without prior authentication.

The database includes sensitive data like passwords, card pins, encrypted Mifare sitekeys and much more.

- Classification / Type
    - CWE-285: Improper Authorization
- CVSS Vector:
    - CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:A/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N
- Base Score: 5.9 (Medium)
- Estimated Risk: Medium
- Affected Versions:
    - 92xx-K5: All Versions older than XAMB 04.06.212 RA
- Mitigation Details:
    - 92xx-K5:

      To secure the Access Manager 92xx, it is highly recommended to update to the latest FW, at least XAMB 04.06.212 RA.

CVE-2025-59101 Insufficient Session Management

Instead of typical session tokens or cookies, it is verified on a per-request basis if the originating IP address has once successfully logged in. As soon as an authentication request from a certain source IP is successful, the IP address is handled as authenticated. No other session information is stored. Therefore, it is possible to spoof the IP address of a logged-in user to gain access to the Access Manager web interface.

- Classification / Type
    - CWE-291: Reliance on IP Address for Authentication
- CVSS Vector:
    - CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
- Base Score: 7.7 (High)
- Estimated Risk: High
- Affected Versions:
    - 92xx-K5: All Versions older than XAMB 04.06.212 RA
    - 92xx-K7: All Versions older than BAME 04.07.268 RA
- Mitigation Details:
    - 92xx-K5:

      To secure the Access Manager 92xx, it is highly recommended to update to the latest FW, at least XAMB 04.06.212 RA.
    - 92xx-K7:

      To secure the Access Manager 92xx, it is highly recommended to update to the latest FW, at least BAME 04.07.268 RA.

CVE-2025-59102 Secrets Stored in Plaintext in Database

The web server of the Access Manager offers a functionality to download a backup of the local database stored on the device. This database contains the whole configuration. This includes encrypted MIFARE keys, card data, user PINs and much more. The PINs are even stored unencrypted. Combined with the fact that an attacker can easily get access to the backup functionality by abusing the session management issue (CVE-2025-59101), or by exploiting the weak default password (CVE-2025-59108), or by simply setting a new password without prior authentication via the SOAP API (CVE-2025-59097), it is easily possible to access the sensitive data on the device.

- Classification / Type
  - CWE-312: Cleartext Storage of Sensitive Information
- CVSS Vector:
  - CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N
- Base Score: 6.9 (Medium)
- Estimated Risk: High
- Affected Versions:
  - 92xx-K5: All Versions older than XAMB 04.06.212 RA
- Mitigation Details:
  - 92xx-K5:

    To secure the Access Manager 92xx, it is highly recommended to update to the latest FW, at least XAMB 04.06.212 RA.

CVE-2025-59103 Weak Default Passwords for SSH Access

The Access Manager 9200 in hardware revision K7 is based on Linux instead of Windows CE embedded in older hardware revisions. In this new hardware revision, it was noticed that an SSH service is exposed on port 22. By analyzing the firmware of the devices, it was noticed that there are two users with hardcoded and weak passwords that can be used to access the devices via SSH. The passwords can be also guessed very easily. The password of at least one user is set to a random value after the first deployment, with the restriction that the password is only randomized if the configured date is prior to 2022. Therefore, under certain circumstances, the passwords are not randomized. For example, if the clock is never set on the device, the battery of the clock module has been changed, the Access Manager has been factory reset and has not received a time yet.

- Classification / Type
  - CWE-1391: Use of Weak Credentials
- CVSS Vector:
  - CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

- Base Score: 9.2 (Critical)
- Estimated Risk: Medium
- Affected Versions:
  - 92xx-K7: All Versions older than BAME 05.01.88 RA
- Mitigation Details:
  - 92xx-K7:

    It is recommended to update the Access Manager 92xx K7 at least to the firmware version BAME 05.01.88 RA.

CVE-2025-59104 Unlocked Bootloader

With physical access to the device and enough time an attacker is able to solder test leads to the debug footprint (or use the 6-Pin tag-connect cable). Thus, the attacker gains access to the bootloader, where the kernel command line can be changed. An attacker is able to gain a root shell through this vulnerability.

- Classification / Type
  - CWE-1234: Hardware Internal or Debug Modes Allow Override of Locks
- CVSS Vector:
  - CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
- Base Score: 7.0 (High)
- Estimated Risk: High
- Affected Versions:
  - 92xx-K7: All Versions older than BAME 06.00 RA
- Mitigation Details:
  - 92xx-K7:

    A firmware update to at least BAME 06.00 RA is highly recommended. Hardware access and special equipment are required to exploit this vulnerability. In general, the Access Manager should be installed in a secured area and protected by a tamper contact.

CVE-2025-59105 Unencrypted Flash Storage

With physical access to the device and enough time an attacker can desolder the flash memory, modify it and then reinstall it because of missing encryption. Thus, essential files, such as "/etc/passwd", as well as stored certificates, cryptographic keys, stored PINs and so on can be modified and read, in order to gain SSH root access on the Linux-based K7 model. On the Windows CE based K5 model, the password for the Access Manager can additionally be read in plain text from the stored SQLite database.

- Classification / Type
  - CWE-312: Cleartext Storage of Sensitive Information
- CVSS Vector:
  - CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
- Base Score: 7.0 (High)
- Estimated Risk: Medium
- Affected Versions:
  - 92xx-K5: All Versions
  - 92xx-K7: All Versions older than BAME 06.00 RA
- Mitigation Details:
  - 92xx-K5:

    This cannot be fixed by the firmware. Hardware access and special equipment are required to exploit this vulnerability. In general, the Access Manager should be installed in a secured area and protected by a tamper contact.
  - 92xx-K7:

    A firmware update to at least BAME 06.00 RA is recommended. Hardware access and special equipment are required to exploit this vulnerability. In general, the Access Manager should be installed in a secured area and protected by a tamper contact.

CVE-2025-59106 Web Server Running with Root Privileges

The binary serving the web server and executing basically all actions launched from the Web UI is running with root privileges. This is against the least privilege principle. If an attacker is able to execute code on the system via other vulnerabilities it is possible to directly execute commands with highest privileges.

- Classification / Type
  - CWE-272: Least Privilege Violation
- Base Score: - (Low)
- Estimated Risk: Low
- Affected Versions:
  - 92xx-K7: All Versions older than BAME 06.00 RA
- Mitigation Details:
  - 92xx-K7:

    To secure the devices from unauthorized access, it is highly recommended to change the default password and update to at least firmware version BAME 06.00 RA.

CVE-2025-59107 Static Firmware Encryption Password

Dormakaba provides the software FWServiceTool to update the firmware version of the Access Managers via the network. The firmware in some instances is provided in an encrypted ZIP file. Within this tool, the password used to decrypt the ZIP and extract the firmware is set statically and can be extracted. This password was valid for multiple observed firmware versions.

- Classification / Type
  - CWE-798: Use of Hard-coded Credentials
- CVSS Vector:
  - CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N
- Base Score: 8.5 (High)
- Estimated Risk: Low
- Affected Versions:
  - 92xx-K5: All Versions
- Mitigation Details:
  - 92xx-K5:

    No measures needed. This will not be fixed. The K5 device is discontinued and should be replaced by a K7 device.

CVE-2025-59108 Weak Default Passwords

By default, the password for the Access Manager's web interface is set to 'admin'. In the tested version changing the password was not enforced.

- Classification / Type
  - CWE-1392: Use of Default Credentials
- CVSS Vector:
  - CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
- Base Score: 9.2 (Critical)
- Estimated Risk: High
- Affected Versions:
  - 92xx-K5: All Versions
  - 92xx-K7: All Versions older than BAME 04.07.268 RA
- Mitigation Details:
  - 92xx-K5:

    To secure the devices from unauthorized access, it is highly recommended to change the default password.
  - 92xx-K7:

    To secure the devices from unauthorized access, it is highly recommended to change the default password and update to at least firmware version BAME 06.00 RA.

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
- product.security@dormakaba.com
- https://sec-consult.com/en/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 v3.1 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.