dormakaba

Vulnerabilities in dormakaba products

The dormakaba registration Unit 9002 Generation K5 in older Versions is affected by a vulnerability.

To exploit the vulnerability, an attacker would need access to the hardware.

Advisory Information

ID:	DKSA-26-26-013	
CVE Numbers and Scores:	CVE-2025-59109	5.1 (Medium)
Published:	26 January 2026	
Advisory Version:	1	

Affected Products

- dormakaba registration unit 90 02
    - All Versions older than FW 0039
    - Serial number older than: 0700039…

Mitigations

The vulnerability can only be exploited with physical access to the device, special equipment and by reinstalling a manipulated device.

To limit the manipulability of the device, a newer version of the 9002 (Serial number starts with: 0700039…) can be installed.

The version of the installed registration unit can only be checked on site!

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-2025-59109 UART Leaking Sensitive Data

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-1295: Debug Messages Revealing Unnecessary Information
- CVSS Vector:
  - CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:A/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N
- Base Score: 5.1 (Medium)
- Estimated Risk: Medium
- Affected Versions: All Versions older than FW 0039,
  Serial number older than: 0700039…
- Mitigation Details:
  - The vulnerability can only be exploited with physical access to the device, special equipment and by reinstalling a manipulated device. To limit the manipulability of the device, a newer version of the 9002 (Serial number starts with: 0700039…) can be installed. The version of the installed detection unit can only be checked on site!

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.