Vulnerability in dormakaba evolo Service

Installations of the dormakaba evolo Service are affected by a vulnerability. The evolo Service is needed for using Terminals for CardLink Updates together with the Access Control Solution dormakaba evolo Manager (KEM).

To exploit these vulnerabilities, an attacker would need prior access to the network in which the machine with the service is operating. Exploitation is only possible from within the internal network.

CVE ID is requested and pending.

Advisory Information

ID:	DKSA-26-31-031	
CVE Numbers and Scores:	*pending*	9.3 (Critical)
Published:	31 March 2026	
Advisory Version:	1	

Affected Products

- dormakaba evolo Service
  - All Versions

Mitigations

If no CardLink Update Terminals are being used the service should be deinstalled completely. All KEM (dormakaba evolo Manager) installations without this service are not affected.

If you need the service then the following recommendations should be followed:

- Operate the machine with the service in a protected network
- Limit the access to the server by strict firewall rules

Recommendation

	Risk	Recommendation
☑	**High/Critical**	Mitigations 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-*pending* Unauthenticated remote code execution

The dormakaba evolo Service is a Windows service based on .NET remoting. This technology is insecure, allowing any unauthenticated attacker that can reach the service to execute arbitrary code as SYSTEM.

- Classification / Type
  - CWE-502: Deserialization of Untrusted Data
- CVSS Vector:
  - CVSS: 4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:N
- Base Score: 9.3 (Critical)
- Risk Assessment: Critical
- Affected Versions: All Versions
- Mitigation Details:
  - Operate the machine running the service only in a protected network without any external connectivity.
  - Activate a firewall on the machine and restrict any incoming traffic to only the Terminals that are being used as CardLink Update stations. All other traffic should be completely blocked.

Additional Information

Legal Disclaimer

Please ensure that your security measures comply with relevant regulatory requirements, including privacy and notification obligations.

Terms of Use

Additional Resources

- https://dormakabagroup.com/en/security
- securitysupport@dormakaba.com

Appendix

Acknowledgements

dormakaba thanks Hans-Martin Münch from MOGWAI LABS GmbH for responsibly disclosing this issue and for his 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).