PHP2Shell Vulnerabilities

On 20 October 2026, information about two critical vulnerabilities in the PHP interpreter, known as PHP2Shell (CVE-2026-109618 and CVE-2026-109619), became public. On 21 October 2026, the PHP project released security updates addressing these vulnerabilities. Successful exploitation can allow an unauthenticated attacker to execute arbitrary code remotely on a server running a vulnerable PHP version.

Based on the technical assessments completed by the responsible product and service organizations as of 23 October 2026, the dormakaba system solutions listed in this advisory are not affected by CVE-2026-109618 or CVE-2026-109619.

No dormakaba product-specific action is required for the system solutions listed in this advisory.

Customers operating separate PHP-based applications or infrastructure should assess and update those environments in accordance with the applicable PHP or platform-vendor guidance.

Advisory Information

ID:	DKSA-26-23-101	
CVE Numbers and Scores:	CVE-2026-109618	9.2 (Critical)
	CVE-2026-109619	9.2 (Critical)
Published:	23 October 2026	
Advisory Version:	1	

Not Affected Products

- Kaba exos 9300
- dormakaba MATRIX (MATRIX ONE, MATRIX Professional, MATRIX Cloud)
- dormakaba evolo Manager
- dormakaba evolo smart
- dormakaba exivo
- dormakaba resivo

- dormakaba B-COMM
- dormakaba B-COMM HCM/7/ERP
- dormakaba skyra
- dormakaba EntriWorX
- Keyscan Aurora and Keyscan LUNA
- Ambiance and Community
- dormakaba Safe Locks (Axessor, Apexx, Paxos, Cencon)
- dormakaba Wi-Q
- dormakaba Lyazon

The assessment covers the associated components and services that form part of the listed dormakaba system solutions, including applicable access managers, terminals, gateways and cloud services. It does not cover separately operated customer infrastructure or third-party applications.

Mitigations

Because the dormakaba system solutions listed in this advisory are not affected, no dormakaba product-specific mitigation is required.

Customers operating separate PHP-based applications or infrastructure should update affected PHP installations to version 8.2.35, 8.3.36, 8.4.27 or 8.5.12, as applicable to the respective PHP release branch, or install the corresponding security update provided by their platform vendor. For externally hosted environments, customers should confirm that the responsible hosting or service provider has applied the relevant security update. Unsupported PHP versions should be migrated to a supported and patched release.

Recommendation

The recommendation rating below applies to the dormakaba system solutions listed in this advisory.

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

PHP is a widely used scripting language for web applications. The vulnerabilities are located in the PHP interpreter itself and not in individual applications. PHP released fixed versions on 21 October 2026. Exploitation attempts have been reported.

CVE-2026-109618 Remote Code Execution via Out-of-Memory Corruption

Out-of-memory handling can interrupt PHP while internal request data is only partially initialized. Request cleanup may then treat the invalid data as valid, which can lead to remote code execution by an unauthenticated attacker.

- Base Score: 9.2 (Critical, CVSS v4.0)
- Affected PHP Versions:
    - All versions before 8.2.35, 8.3.36, 8.4.27 and 8.5.12. Older, unsupported PHP branches are also affected.
- Status of dormakaba System Solutions:
    - Not affected. See Section Not Affected Products.

CVE-2026-109619 Remote Code Execution via Stale Global State

Request-owned internal state can survive after its backing memory has been freed. A later request handled by the same worker may use this stale state before normal initialization resets it. This can lead to remote code execution and disclosure of memory contents by an unauthenticated attacker.

- Base Score: 9.2 (Critical, CVSS v4.0)
- Affected PHP Versions:
    - All versions before 8.2.35, 8.3.36, 8.4.27 and 8.5.12. Older, unsupported PHP branches are also affected.
- Status of dormakaba System Solutions:
    - Not affected. See Section Not Affected Products.

Additional Information

Legal Disclaimer

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

Terms of Use

This content is licensed under the Creative Commons Attribution 4.0 International License (https://creativecommons.org/licenses/by/4.0/). If you distribute this content, or a modified version of it, you must provide attribution to dormakaba and provide a link to the original.

Additional Resources

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

Appendix

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.