BIZERBA-SA-2026-0005: PHP2Shell

Publisher: Bizerba SE & Co. KG	Document category: csaf_security_advisory
Initial release date: 2026-11-09T14:00:00.000Z	Engine: Secvisogram 2.6.17
Current release date: 2026-11-09T14:00:00.000Z	Build Date: 2026-11-12T15:11:08.654Z
Current version: 1	Status: final
CVSSv3.1 Base Score: 9	Severity:
Original language:	Language: en-us
Also referred to:	

CVSS Scoring

Vulnerability classification has been performed using the CVSS v3.1 scoring system . The CVSS environmental score is specific to each customer’s environment and should be defined by the customer to attain a final scoring.

Vulnerabilities

RCE via OOM corruption (CVE-2026-124846)

RCE via OOM corruption

Under certain conditions, an unauthenticated remote attacker could exploit CVE-2026-109618 or CVE-2026-109619 by sending specially crafted requests to the RDM web service. Successful exploitation could allow the attacker to run arbitrary code with the privileges of the web server or PHP process, potentially accessing, modifying or deleting data, or disrupting the RDM service.

CWE:	CWE-416:Use After Free

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
RDM < PHP 8.2	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H	9

Fixed

- all installations > PHP 8.2

Remediations

Mitigation (2026-11-09T11:00:00.000Z)

Update to PHP Version 8.2.35

For products:

- RDM < PHP 8.2

Bizerba SE & Co. KG

Namespace: https://www.bizerba.com/de/de/familien-unternehmen-seit-1866/corporate-governance-verantwortungsvoll-global-handeln/bizerba-security-informationen

security@bizerba.com

References

- Bizerba Security Advisorys https://www.bizerba.com/de/de/familien-unternehmen-seit-1866/corporate-governance-verantwortungsvoll-global-handeln/bizerba-security-informationen (https://www.bizerba.com/de/de/familien-unternehmen-seit-1866/corporate-governance-verantwortungsvoll-global-handeln/bizerba-security-informationen)

Revision history

Version	Date of the revision	Summary of the revision
1	2026-11-09T14:00:00.000Z	Release

Sharing rules

TLP:WHITE
For the TLP version see: https://us-cert.cisa.gov/tlp/ (https://us-cert.cisa.gov/tlp/)

Security Update Information

With respect to Directive (EU) 2019/770 and Directive (EU) 2019/771 and their national transposition laws, please note:

It is your responsibility to download and/or install any security updates provided by us, for example to maintain product or data security. If you fail to install a security update provided to you within a reasonable period of time, we will not be liable for any product defect solely due to the absence of such security update.

Alternatively, we are entitled to directly download and/or install security updates regardless of your settings. In these cases, we will provide you with the relevant information, e.g. in this security advisory.