Remote Code Execution in mpGabinet

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-40552
State	PUBLISHED
Assigner	CERT-PL
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-28 14:16:13 UTC
Updated	2026-04-28 20:20:09 UTC
Description	mpGabinet is vulnerable to Remote Command Execution. An authorized user with access to the application and direct acce

Risk And Classification

Primary CVSS: v4.0 4.7 MEDIUM from cvd@cert.pl

CVSS:4.0/AV:A/AC:L/AT:N/PR:H/UI:P/VC:L/VI:L/VA:L/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-669 | CWE-669 CWE-669: Incorrect Resource Transfer Between Spheres

Version	Source	Type	Score	Severity	Vector
4.0	cvd@cert.pl	Secondary	4.7	MEDIUM	CVSS:4.0/AV:A/AC:L/AT:N/PR:H/UI:P/VC:L/VI:L/VA:L/SC:H/SI:H/SA:H/E:X/C...
4.0	CNA	CVSS	4.7	MEDIUM	CVSS:4.0/AV:A/AC:L/AT:N/PR:H/UI:P/VC:L/VI:L/VA:L/SC:H/SI:H/SA:H

CVSS v4.0 Breakdown

Attack Vector

Adjacent

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

Passive

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:A/AC:L/AT:N/PR:H/UI:P/VC:L/VI:L/VA:L/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	BinSoft	MpGabinet	affected 23.12.19 semver	Not specified

References

Reference	Source	Link	Tags
cert.pl/posts/2026/04/CVE-2026-40550	cvd@cert.pl	cert.pl	
www.mpgabinet.pl	cvd@cert.pl	www.mpgabinet.pl	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Robert Kruczek (en)

CNA: Kamil Szczurowski (en)

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**