

Security Advisory

Geutebrück GmbH • Im Nassen 7-9 • 53578 Windhagen

Unauthenticated Access to GCoreServer Database and Recorded Media

Advisory ID	GBSA-2026-001
CVE ID	CVE-2026-78988
Published	2026-06-10
Last Updated	2026-10-01
Affected Product	G-Core
Affected Component	GCoreServer
Severity	High
CVSS v3.1 Base Score	7.7
CVSS v3.1 Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:H
CWE	CWE-306 - Missing Authentication for Critical Function

Summary

Geutebrueck has identified and remediated an authentication enforcement issue in GCoreServer. A remote attacker with network access to the GCoreServer may be able to interact with protected server functionality without completing the expected authentication sequence.

Internal validation demonstrated that an unauthenticated client can access database query functionality and retrieve stored media data from the server. This may expose video recordings, channel metadata, event data, and other operational contents.

Customers should restrict network access to trusted networks and apply the relevant security update for their product track.

Severity Assessment

CVSS v3.1 Base Score: 7.7 (High)

CVSS v3.1 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:H

Remediation

Apply the security update for the affected G-Core product track as soon as possible. The updated version is available for download in the Geutebrueck Partner Portal. If you require assistance obtaining or applying the update, please contact service@geutebrueck.com.

Geutebrück GmbH

Im Nassen 7-9
53578 Windhagen

Telefon +49 2645 137-0
Fax +49 2645 137-999
Mail info@geutebrueck.com

Commerzbank

IBAN DE15 3804 0007 0119 9660 00
BIC COBADEFFXXX

Deutsche Bank

IBAN DE48 3807 0059 0221 1563 00
BIC DEUTDE33XXX

Handelsregister Montabaur

HRB 14475
Ust-ID DE813443473

Geschäftsleitung

Katharina Geutebrück
Christoph Hoffmann

Workarounds

1. Restrict network access to trusted administrative networks only.
2. Block GCoreServer from public internet access and untrusted network segments.
3. Place GCoreServer systems behind VPN, firewall, or bastion-controlled access where operationally possible.
4. Review firewall rules and network segmentation for all access paths to GCoreServer systems.
5. Monitor for unexpected connections from untrusted or unusual source addresses.

Network isolation is a workaround only. It does not remove the vulnerability from affected software versions.

Exploitation Status

Geutebrueck has validated functional exploitation internally. As of this publication date, exploitation in the wild has not been confirmed.

Credits

This vulnerability was identified during internal Geutebrueck security assessment activities.

Contact

For questions regarding this advisory or to report a security issue, please contact the Geutebrueck security team at security@geutebrueck.com.

Legal Notice

The information provided in this advisory is provided "as is" without warranty of any kind. Geutebrueck GmbH disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Geutebrueck GmbH be liable for any damages arising from the use of or inability to use this information.

Affected Products

Product / Track	Affected Versions	Fixed Version	Status
G-Core	All versions before 8.3.2	8.3.2	Fix available
G-Core	All versions before 9.1	9.1	Fix available

Revision History

Version	Date	Description
1.1	2026-10-01	CVE added; summary wording clarified
1.0	2026-06-10	Public advisory release