



IQSIGHT-SA-261342: BVMS Possible Information Disclosure

Severity: 8.7
Publication Date: 2026-09-30
Last Updated: 2026-09-30
Current Version: 1.0

Summary

This advisory addresses a critical security concern regarding potential information disclosure risks. Recent assessments have indicated that certain trust anchors within BVMS systems may be at risk of compromise. This situation could lead to unauthorized access to sensitive data, man-in-the-middle attacks, and other forms of information disclosure. Attackers may exploit these vulnerabilities to intercept or manipulate data transmitted over secure channels.

Affected Products

Product(s)	Vulnerability(ies)	Version(s)
IQSIGHT BVMS	CVE-2026-10764	4.5 <= 12.3
IQSIGHT BVMS Viewer	CVE-2026-10764	4.5 <= 12.3
IQSIGHT DIVAR IP 7000 R2	CVE-2026-10764	6.0 <= 12.0.1
IQSIGHT DIVAR IP all-in-one 4000	CVE-2026-10764	11.1.1 <= 12.3
IQSIGHT DIVAR IP all-in-one 5000	CVE-2026-10764	9.0 <= 12.3
IQSIGHT DIVAR IP all-in-one 6000	CVE-2026-10764	11.1.1 <= 12.3
IQSIGHT DIVAR IP all-in-one 7000	CVE-2026-10764	9.0 <= 12.3
IQSIGHT DIVAR IP all-in-one 7000 R3	CVE-2026-10764	10.1.1 <= 12.3
IQSIGHT DIVAR IP all-in-one 7000 R4	CVE-2026-10764	12.1 <= 12.3

Vulnerability Details

CVE-2026-10764

Information disclosure in BVMS 4.5 up to 12.3 including allows man-in-the-middle attackers to gain unauthorized access to sensitive data.

- CWE-321: Use of Hard-coded Cryptographic Key
- CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N
- Base Score: 8.7

Solution and Mitigations

Solution

Software update

Install or upgrade to at least BVMS 13.0

Mitigation

BVMS installations

Execute "BVMS_SecurityUpdate_01" tool

Ensure that all Microsoft patches and updates, including OS updates, are installed. Execute "BVMS_SecurityUpdate_01" on all BVMS servers, all client hosts, and all hosts where either the BVMS server or BVMS client is installed, restart all BVMS services or restart the machine.

If an install, repair, or modify action of the affected BVMS setup is performed, "BVMS_SecurityUpdate_01" must be executed again afterward. A prerequisite for "BVMS_SecurityUpdate_01" is that .NET Framework 4.8 is installed.

Install latest cumulative Patch (required only for OIDC feature in BVMS 12.2)

BVMS 12.2: Install patch "BVMS1220296_Patch_Cum11.zip" only in case the tool "BVMS_SecurityUpdate_01" was used and OIDC feature is in use, restart all BVMS services or restart the machine.

DIVAR systems

Open the folder with the patch file BVMS_SecurityUpdate_01.exe

Double-click BVMS_SecurityUpdate_01.exe to start the update.

In the Windows User Account Control (UAC), click Yes.

Wait until the update process finishes.

If the installation is successful a pop-up message will be displayed with the message:

"Update succeeded"

Click OK to close the message.

The patch installation is now complete.

Restart all BVMS services or restart the machine.

Additional Resources

- BVMS Download Area: <https://downloadstore.keenfinity-group.com/index.php?type=BVMS>
- BVMS Viewer Download Area: <https://downloadstore.keenfinity-group.com/index.php?type=BVMSVWR>

Appendix

Fixes for the Affected Products

BVMS

Affected versions	Version or patch that fixes the vulnerability
from 4.5 up to 12.3 (including)	Use tool "BVMS_SecurityUpdate_01" or upgrade to 13.0 or higher version.

BVMS Download Area

BVMS Viewer

Affected versions	Version or patch that fixes the vulnerability
from 4.5 up to 12.3 (including)	Use tool "BVMS_SecurityUpdate_01" or upgrade to 13.0 or higher version.

BVMS Viewer Download Area

DIVAR IP all-in-one 7000 R3

Affected BVMS versions	Version or patch that fixes the vulnerability
up to 12.3 (including)	Use tool "BVMS_SecurityUpdate_01" or upgrade to 13.0 or higher version.

BVMS Download Area

DIVAR IP 7000 R2

Affected BVMS versions	Version or patch that fixes the vulnerability
up to 12.0.1 (including)	Use tool "BVMS_SecurityUpdate_01".

BVMS Download Area

DIVAR IP all-in-one 4000

Affected BVMS versions	Version or patch that fixes the vulnerability
up to 12.3 (including)	Use tool "BVMS_SecurityUpdate_01" or upgrade to 13.0 or higher version.

BVMS Download Area

DIVAR IP all-in-one 5000

Affected BVMS versions	Version or patch that fixes the vulnerability
up to 12.3 (including)	Use tool "BVMS_SecurityUpdate_01" or upgrade to 13.0 or higher version.

BVMS Download Area

DIVAR IP all-in-one 6000

Affected BVMS versions	Version or patch that fixes the vulnerability
up to 12.3 (including)	Use tool "BVMS_SecurityUpdate_01" or upgrade to 13.0 or higher version.

BVMS Download Area

DIVAR IP all-in-one 7000

Affected BVMS versions	Version or patch that fixes the vulnerability
up to 12.3 (including)	Use tool "BVMS_SecurityUpdate_01" or upgrade to 13.0 or higher version.

BVMS Download Area

DIVAR IP all-in-one 7000 R4

Affected BVMS versions	Version or patch that fixes the vulnerability
from 10.1.1 up to 12.3 (including)	Use tool "BVMS_SecurityUpdate_01" or upgrade to 13.0 or higher version.

BVMS Download Area

Material Lists

BVMS

Family Name	CTN	SAP#	Material description
BVMS Professional	MBV-BPRO	F.01U.393.647	License Professional base
BVMS Plus	MBV-BPLU	F.01U.393.650	License Plus base
BVMS Plus DIP	MBV-BPLU-DIP	F.01U.374.503	License Plus base for DIVAR IP
BVMS Lite	MBV-BLIT	F.01U.393.648	License Lite base
BVMS Lite DIP	MBV-BLIT-DIP	F.01U.358.975	License Lite base for DIVAR IP

DIVAR IP all-in-one 4000

Family Name	CTN	SAP#	Material description
DIVAR IP all-in-one 4000	DIP-4420IG-00N	F.01U.404.040	Management appliance w/o HDD
DIVAR IP all-in-one 4000	DIP-4424IG-2HD	F.01U.404.041	Management appliance 2×4TB
DIVAR IP all-in-one 4000	DIP-4428IG-2HD	F.01U.404.042	Management appliance 2×8TB
DIVAR IP all-in-one 4000	DIP-442IIG-2HD	F.01U.404.043	Management appliance 2×18TB

DIVAR IP all-in-one 5000

Family Name	CTN	SAP#	Material description
DIVAR IP all-in-one 5000	DIP-5240IG-00N	F.01U.361.821	Management Appliance w/o HDD
DIVAR IP all-in-one 5000	DIP-5244IG-4HD	F.01U.362.424	Management Appliance 4×4TB
DIVAR IP all-in-one 5000	DIP-5248IG-4HD	F.01U.362.423	Management Appliance 4×8TB
DIVAR IP all-in-one 5000	DIP-524CIG-4HD	F.01U.362.422	Management Appliance 4×12TB
DIVAR IP all-in-one 5000	DIP-5240GP-00N	F.01U.359.551	Management Appliance GPU wo HD
DIVAR IP all-in-one 5000	DIP-5244GP-4HD	F.01U.359.552	Management Appliance GPU 4×4TB
DIVAR IP all-in-one 5000	DIP-5248GP-4HD	F.01U.359.553	Management Appliance GPU 4×8TB
DIVAR IP all-in-one 5000	DIP-524CGP-4HD	F.01U.359.554	Management Appliance GPU 4×12TB

DIVAR IP all-in-one 6000

Family Name	CTN	SAP#	Material description
DIVAR IP all-in-one 6000	DIP-6440IG-00N	F.01U.404.045	Management appliance 1U w/o HDD
DIVAR IP all-in-one 6000	DIP-6444IG-4HD	F.01U.404.046	Management appliance 1U 4×4TB
DIVAR IP all-in-one 6000	DIP-6448IG-4HD	F.01U.404.047	Management appliance 1U 4×8TB
DIVAR IP all-in-one 6000	DIP-644IIG-4HD	F.01U.404.048	Management appliance 1U 4×18TB

DIVAR IP all-in-one 7000

Family Name	CTN	SAP#	Material description
DIVAR IP all-in-one 7000	DIP-7280-00N	F.01U.362.591	2U Management Appliance w/o HD
DIVAR IP all-in-one 7000	DIP-7284-8HD	F.01U.362.592	2U Management Appliance 8×4TB
DIVAR IP all-in-one 7000	DIP-7288-8HD	F.01U.362.593	2U Management Appliance 8×8TB
DIVAR IP all-in-one 7000	DIP-728C-8HD	F.01U.362.594	2U Management Appliance 8×12TB
DIVAR IP all-in-one 7000	DIP-72G0-00N	F.01U.362.595	3U Management Appliance wo HDD
DIVAR IP all-in-one 7000	DIP-72G8-16HD	F.01U.362.596	3U Management Appliance 16×8TB
DIVAR IP all-in-one 7000	DIP-72GC-16HD	F.01U.362.597	3U Management Appliance 16×12T
DIVAR IP all-in-one 7000	DIP-7380-00N	F.01U.385.539	Management appliance 2U without HD
DIVAR IP all-in-one 7000	DIP-7384-8HD	F.01U.385.540	Management appliance 2U 8X4TB
DIVAR IP all-in-one 7000	DIP-7388-8HD	F.01U.385.541	Management appliance 2U 8X8 TB
DIVAR IP all-in-one 7000	DIP-738C-8HD	F.01U.385.542	Management appliance 2U 8X12 TB
DIVAR IP all-in-one 7000	DIP-73G0-00N	F.01U.385.543	Management appliance 3U without HD
DIVAR IP all-in-one 7000	DIP-73G8-16HD	F.01U.385.544	Management appliance 3U 16X8TB
DIVAR IP all-in-one 7000	DIP-73GC-16HD	F.01U.385.545	Management appliance 3U 16X12 TB
DIVAR IP all-in-one 7000	DIP-74C0-00N	F.01U.417.248	Management appliance, 2U w/o HDD
DIVAR IP all-in-one 7000	DIP-74C4-8HD	F.01U.417.249	Management appliance, 2U 8X4TB
DIVAR IP all-in-one 7000	DIP-74C8-8HD	F.01U.417.250	Management appliance, 2U 8X8TB
DIVAR IP all-in-one 7000	DIP-74CI-8HD	F.01U.417.251	Management appliance, 2U 8X18TB
DIVAR IP all-in-one 7000	DIP-74CI-12HD	F.01U.417.252	Management appliance, 2U 12X18TB
DIVAR IP all-in-one 7000	DIP-74G0-00N	F.01U.417.253	Management appliance, 3U w/o HDD
DIVAR IP all-in-one 7000	DIP-74GI-16HD	F.01U.417.254	Management appliance, 3U 16X18TB

DIVAR IP 7000 R2

Family Name	CTN	SAP#	Material description
DIVAR IP 7000 R2	DIP-7180-00N	F.01U.314.520	DIVAR IP 7000 2U w/o HDD
DIVAR IP 7000 R2	DIP-7183-4HD	F.01U.314.521	DIVAR IP 7000 2U 4×3TB
DIVAR IP 7000 R2	DIP-7183-8HD	F.01U.314.522	DIVAR IP 7000 2U 8×3TB

Family Name	CTN	SAP#	Material description
DIVAR IP 7000 R2	DIP-7184-4HD	F.01U.314.523	DIVAR IP 7000 2U 4×4TB
DIVAR IP 7000 R2	DIP-7184-8HD	F.01U.314.524	DIVAR IP 7000 2U 8×4TB
DIVAR IP 7000 R2	DIP-71F0-00N	F.01U.314.525	DIVAR IP 7000 3U w/o HDD
DIVAR IP 7000 R2	DIP-71F3-16HD	F.01U.314.526	DIVAR IP 7000 3U 16×3TB
DIVAR IP 7000 R2	DIP-71F4-16HD	F.01U.314.527	DIVAR IP 7000 3U 16×4TB
DIVAR IP 7000 R2	DIP-7186-8HD	F.01U.329.143	DIVAR IP 7000 2U 8×6TB
DIVAR IP 7000 R2	DIP-7188-8HD	F.01U.329.144	DIVAR IP 7000 2U 8×8TB
DIVAR IP 7000 R2	DIP-71F6-16HD	F.01U.329.145	DIVAR IP 7000 3U 16×6TB
DIVAR IP 7000 R2	DIP-71F8-16HD	F.01U.329.146	DIVAR IP 7000 3U 16×8TB
DIVAR IP 7000 R2	DIP-7184-8HD-WAG	F.01U.343.277	DIVAR IP 7000 2U 8×4TB, WAG Kit

Remarks

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.

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.

Contact

Please contact IQSIGHT PSIRT if you have feedback, comments, or additional information about this vulnerability at psirt@iqsight.com.

Revision History

Version	Date	Description
1.0	30/09/26	Initial version