

KSA-254356: BVMS Unrestricted SSH Resource Consumption

Severity: 7.5
Publication Date: 2025-08-27
Last Updated: 2025-08-27
Current Version: 1.0

Summary

BVMS SSH Server, while providing secure remote access, can be susceptible to resource consumption issues that can impact server performance and potentially lead to denial-of-service conditions. The service may become unresponsive or crash due to resource exhaustion, denying service to legitimate users. Affected BVMS versions start from 7.5 and include all versions up to and including 12.3.

Affected Products

Product(s)	Vulnerability(ies)	Version(s)
Bosch BVMS	CVE-2002-20001	7.5 <= 12.3

Vulnerability Details

CVE-2002-20001

- CWE-400: Uncontrolled Resource Consumption
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
- Base Score: 7.5

Solution and Mitigations

Software Updates

The recommended approach is to update the software to a fixed version as soon as possible. Please check the Appendix for a list of updated versions for each affected

product.

Secure Network Resources

It is advised to protect network access to BVMS SSH Server. Network administrators should implement the following recommendations in conjunction with laws, regulations, and industry best practices:

- Segment and segregate networks
- Monitor the network and review logs
- Monitor resource usage and implement automated alerts for abnormal behavior on BVMS SSH Server
- Use firewalls or intrusion prevention systems (IPS) to rate-limit SSH connections, preventing attackers from overwhelming the server with connection attempts.

Additional Resources

- [1] Download Area: <https://downloadstore.keenfinity-group.com/index.php?type=BVMS>
- [2] BVMS Appliances (DIVAR IP) Download Area: <https://downloadstore.keenfinity-group.com/index.php?type=DIPBVMS>

Appendix

Fixes for the Affected Products

BVMS

Affected versions	Version or patch that fixes the vulnerability
12.3	BVMS1230171_Patch_Cum4_Sec.zip (or a higher BVMS 12.3 cumulative Patchversion)
12.2	BVMS1220296_Patch_Cum8_Sec.zip (or a higher BVMS 12.2 cumulative Patchversion)
12.1	BVMS1210414_Patch_Cum21_Sec.zip (or a higher BVMS 12.1 cumulative Patchversion)

BVMS Download Area

DIVAR IP all-in-one 4000

Affected BVMS versions	Version or patch that fixes the vulnerability
------------------------	---

Affected BVMS versions	Version or patch that fixes the vulnerability
12.3	BVMS_12.3.0_Updates_SystemManager_package_1.5
12.2	BVMS_12.2.0_Updates_SystemManager_package_1.8
12.1	BVMS_12.1.0_Updates_SystemManager_package_1.21

[BVMS Appliances Download Area](#)

Bosch DIVAR IP all-in-one 5000

Affected BVMS versions	Version or patch that fixes the vulnerability
12.3	BVMS_12.3.0_Updates_SystemManager_package_1.5
12.2	BVMS_12.2.0_Updates_SystemManager_package_1.8
12.1	BVMS_12.1.0_Updates_SystemManager_package_1.21

[BVMS Appliances Download Area](#)

DIVAR IP all-in-one 6000

Affected BVMS versions	Version or patch that fixes the vulnerability
12.3	BVMS_12.3.0_Updates_SystemManager_package_1.5
12.2	BVMS_12.2.0_Updates_SystemManager_package_1.8
12.1	BVMS_12.1.0_Updates_SystemManager_package_1.21

[BVMS Appliances Download Area](#)

Bosch DIVAR IP all-in-one 7000

Affected BVMS versions	Version or patch that fixes the vulnerability
12.3	BVMS_12.3.0_Updates_SystemManager_package_1.5
12.2	BVMS_12.2.0_Updates_SystemManager_package_1.8
12.1	BVMS_12.1.0_Updates_SystemManager_package_1.21

[BVMS Appliances Download Area](#)

Material Lists

BVMS

Family Name	CTN	SAP#	Material description
BVMS Professional 12.3	MBV-BPRO	F.01U.393.647	License Professional base
BVMS Plus 12.3	MBV-BPLU	F.01U.393.650	License Plus base

Family Name	CTN	SAP#	Material description
BVMS Plus 12.3 DIP	MBV-BPLU-DIP	F.01U.374.503	License Plus base for DIVAR IP
BVMS Lite 12.3	MBV-BLIT	F.01U.393.648	License Lite base
BVMS Lite 12.3 DIP	MBV-BLIT-DIP	F.01U.358.975	License Lite base for DIVAR IP
BVMS Professional 12.2	MBV-BPRO	F.01U.393.647	License Professional base
BVMS Plus 12.2	MBV-BPLU	F.01U.393.650	License Plus base
BVMS Plus 12.2 DIP	MBV-BPLU-DIP	F.01U.374.503	License Plus base for DIVAR IP
BVMS Lite 12.2	MBV-BLIT	F.01U.393.648	License Lite base
BVMS Lite 12.2 DIP	MBV-BLIT-DIP	F.01U.358.975	License Lite base for DIVAR IP
BVMS Professional 12.1	MBV-BPRO	F.01U.393.647	License Professional base
BVMS Plus 12.1	MBV-BPLU	F.01U.393.650	License Plus base
BVMS Plus 12.1 DIP	MBV-BPLU-DIP	F.01U.374.503	License Plus base for DIVAR IP
BVMS Lite 12.1	MBV-BLIT	F.01U.393.648	License Lite base
BVMS Lite 12.1 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 2x4TB
DIVAR IP all-in-one 4000	DIP-4428IG-2HD	F.01U.404.042	Management appliance 2x8TB
DIVAR IP all-in-one 4000	DIP-442IIG-2HD	F.01U.404.043	Management appliance 2x18TB

Bosch 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 4x4TB

Family Name	CTN	SAP#	Material description
DIVAR IP all-in-one 5000	DIP-5248IG-4HD	F.01U.362.423	Management Appliance 4x8TB
DIVAR IP all-in-one 5000	DIP-524CIG-4HD	F.01U.362.422	Management Appliance 4x12TB
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 4x4TB
DIVAR IP all-in-one 5000	DIP-5248GP-4HD	F.01U.359.553	Management Appliance GPU 4x8TB
DIVAR IP all-in-one 5000	DIP-524CGP-4HD	F.01U.359.554	Management Appliance GPU 4x12TB

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 4x4TB
DIVAR IP all-in-one 6000	DIP-6448IG-4HD	F.01U.404.047	Management appliance 1U 4x8TB
DIVAR IP all-in-one 6000	DIP-644IIG-4HD	F.01U.404.048	Management appliance 1U 4x18TB

Bosch 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 8x4TB
DIVAR IP all-in-one 7000	DIP-7288-8HD	F.01U.362.593	2U Management Appliance 8x8TB
DIVAR IP all-in-one 7000	DIP-728C-8HD	F.01U.362.594	2U Management Appliance 8x12TB
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 16x8TB
DIVAR IP all-in-one 7000	DIP-72GC-16HD	F.01U.362.597	3U Management Appliance 16x12T

Family Name	CTN	SAP#	Material description
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

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.

Revision History

Version	Date	Description
1.0	27-08-2025	First Version

© Keenfinity 2025