Unrestricted resource consumption in BVMS

Advisory Information

- **Advisory ID:**
- **CVE Numbers and CVSS v3.1 Scores:**
  - CVE-2024-0367
    - Base Score:
- **Published:**
- **Last Updated:**

Summary

A vulnerability has been identified in the Bosch VMS Central Server concerning unrestricted resource consumption, leading to excessive use of disk space. The uncontrolled resource consumption can lead to a significant impact on the availability and performance of the affected system. This can result in the inability to store new data, process incoming requests, and perform essential system functions. In severe cases, it may lead to system crashes and data loss.

Affected Products

- Bosch BVMS
  - CVE-2024-0367
    - Versions
- Bosch BVMS Viewer
  - CVE-2024-0367

- Versions(s): 8.0 - 12.0.1 (including)
- Bosch DIVAR IP 7000 R2
  - CVE-2024-0367[8]
    - Versions(s): 8.0 - 12.0.1 (including)
- Bosch DIVAR IP all-in-one 5000
  - CVE-2024-0367[8]
    - Versions(s): 8.0 - 12.0.1 (including)
- Bosch DIVAR IP all-in-one 7000
  - CVE-2024-0367[8]
    - Versions(s): 8.0 - 12.0.1 (including)
- Bosch DIVAR IP all-in-one 7000 R2
  - CVE-2024-0367[8]
    - Versions(s): 10.1 - 12.0.1 (including)
- Bosch DIVAR IP all-in-one 4000
  - CVE-2024-0367[8]
    - Versions(s): 11.1.1 - 12.0.1 (including)
- Bosch DIVAR IP all-in-one 6000
  - CVE-2024-0367[8]
    - Versions(s): 11.1.1 - 12.0.1 (including)

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 Ressources

It is advised to protect network access to Bosch VMS Central 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 Bosch VMS Central Server

Vulnerability Details

CVE-2024-33618

CVE description: Uncontrolled Resource Consumption in Bosch VMS Central Server in Bosch VMS 12.0.1 allows attackers to consume excessive amounts of disk space via network interface.

- Problem Type:
  - CWE-400 Uncontrolled Resource Consumption
- CVSS Vector String: CVSS:4.0/AV:N/AC:L/PR:N/UI:N/VC:N/VI:N/VA:H
  - Base Score: 7.0 (High)

Remarks

Security Update Information

With regard to Directive (EU) 2019/771 and Directive (EU) 2019/770 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, for example, in this security advisory.

CVSS Scoring

Vulnerability classification has been performed using the CVSS v4.0 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.

Additional Resources

- [1] BVMS Download Area: https://downloadstore.boschsecurity.com/index.php?type=BVMS
- [2] BVMS Viewer Download Area: https://downloadstore.boschsecurity.com/index.php?type=BVMSVIEWER
- [3] BVMS Appliances (DIVAR IP): Download Area: https://downloadstore.boschsecurity.com/?type=DIVARIP

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

Revision History

- 16 Oct 2024: Initial Publication

Appendix

Fixes for the Affected Products

BVMS

Affected versions	Version or patch that fixes the vulnerability
12.x.x.x	BVMS_12.0.1.273_Patch_2.0.zip

BVMS Download Area

BVMS Viewer

Affected versions	Version or patch that fixes the vulnerability
12.0.1	[illegible]

[illegible] Viewer Download Area

Bosch DIVAR IP all-in-one 7000 R3

Affected BVMS versions	Version or patch that fixes the vulnerability
12.0.1	BVMS_12.0.1_Updates_SystemManager_package_1.2.zip

[illegible] Appliances Download Area

Bosch DIVAR IP 7000 R2

Affected BVMS versions	Version or patch that fixes the vulnerability
12.0.1	BVMS_12.0.1_Updates_SystemManager_package_1.2.zip

[illegible] Appliances Download Area

Bosch DIVAR IP all-in-one 5000

Affected BVMS versions	Version or patch that fixes the vulnerability
12.0.1	BVMS_12.0.1_Updates_SystemManager_package_1.2.zip

BVMS Appliances Downloads Area

Bosch DIVAR IP all-in-one 7000

Affected BVMS versions	Version or patch that fixes the vulnerability
12.0.1	BVMS_12.0.1_Updates_SystemManager_package_1.2.zip

BVMS Appliances Downloads Area

DIVAR IP all-in-one 4000

Affected BVMS versions	Version or patch that fixes the vulnerability
12.0.1	BVMS_12.0.1_Updates_SystemManager_package_1.2.zip

BVMS Appliances Downloads Area

DIVAR IP all-in-one 5000

Affected BVMS versions	Version or patch that fixes the vulnerability
12.0.1	BVMS_12.0.1_Updates_SystemManager_package_1.2.zip

BVMS Appliances Download Area

Material Lists

BVMS

Family Name	CTN	SAP#	Material description
BVMS Professional 12.0.1	MBV-BPRO	F.01U.390.447	License Professional base
BVMS Plus 12.0.1	MBV-BPLU	F.01U.390.450	License Plus base
BVMS Plus 12.0.1 SAP	MBV-BPLU-SAP	F.01U.374.303	License Plus base for SAP
BVMS Viewer 12.0.1	MBV-BVWR	F.01U.390.449	License Viewer base
BVMS Lite 12.0.1	MBV-BLIT	F.01U.390.448	License Lite base

Family Name	CTN	SAP#	Material description
BVMS Lite 12.0.1 SAP	MBV-BLITE-SAP	F.01U.358.675	License Lite Sales for BVMS IP

Bosch DIVAR IP 7000 R2

Family Name	CTN	SAP#	Material description
DIVAR IP 7000 R2	DIP-7380-00N	F.01U.314.520	DIVAR IP 7000 2U w/o HDD
DIVAR IP 7000 R2	DIP-7380-0HD	F.01U.314.521	DIVAR IP 7000 2U 4xSTB
DIVAR IP 7000 R2	DIP-7380-0HD	F.01U.314.522	DIVAR IP 7000 2U 8xSTB
DIVAR IP 7000 R2	DIP-7380-0HD	F.01U.314.523	DIVAR IP 7000 2U 4xeSTB
DIVAR IP 7000 R2	DIP-7380-0HD	F.01U.314.524	DIVAR IP 7000 2U 8xeSTB
DIVAR IP 7000 R2	DIP-7372-00N	F.01U.314.525	DIVAR IP 7000 2U w/o HDD
DIVAR IP 7000 R2	DIP-7372-16HD	F.01U.314.526	DIVAR IP 7000 2U 16xSTB

Family Name	CTN	SAP#	Material description
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]

Bosch DIVAR IP all-in-one 5000

Family Name	CTN	SAP#	Material description
[illegible]	[illegible]	[illegible]	[illegible]

Family Name	CTN	SAP#	Material description
DIVAR IP all-in-one 5000	DIP-52400I-8HD	F.01U.362.424	Management Appliance 4xHDD
DIVAR IP all-in-one 5000	DIP-52480I-8HD	F.01U.362.423	Management Appliance 4xHDD
DIVAR IP all-in-one 5000	DIP-52401I-8HD	F.01U.362.422	Management Appliance 4x12TB
DIVAR IP all-in-one 5000	DIP-52402P-00N	F.01U.359.557	Management Appliance GPU, w/o HD
DIVAR IP all-in-one 5000	DIP-52402P-8HD	F.01U.359.552	Management Appliance GPU, 4xHDD
DIVAR IP all-in-one 5000	DIP-52480P-8HD	F.01U.359.553	Management Appliance GPU, 4xHDD
DIVAR IP all-in-one 5000	DIP-52401P-8HD	F.01U.359.554	Management Appliance GPU, 4x12TB

Bosch DIVAR IP all-in-one 7000

Family Name	CTN	SAP#	Material description
DIVAR IP all-in-one 7000	DIP-7380-00N	F.01U.362.597	DI Management Appliance w/o HD
DIVAR IP all-in-one 7000	DIP-7384-8HD	F.01U.362.592	DI Management Appliance 8xHDD
DIVAR IP all-in-one 7000	DIP-7388-8HD	F.01U.362.593	DI Management Appliance 8xHDD
DIVAR IP all-in-one 7000	DIP-7381-8HD	F.01U.362.594	DI Management Appliance 8x12TB
DIVAR IP all-in-one 7000	DIP-7332-00N	F.01U.362.595	DI Management Appliance w/o HDD
DIVAR IP all-in-one 7000	DIP-7338-16HD	F.01U.362.596	DI Management Appliance 16xHDD
DIVAR IP all-in-one 7000	DIP-7332-16HD	F.01U.362.597	DI Management Appliance 16x12T

DIVAR IP all-in-one 7000 R3

Family Name	CTN	SAP#	Material description
DIVAR IP all-in-one 7000	DIP 7380 00N	F.01U.385.539	Management appliance 2U without HDD
DIVAR IP all-in-one 7000	DIP 7380 8HD	F.01U.385.540	Management appliance 2U 8HDTB
DIVAR IP all-in-one 7000	DIP 7388 8HD	F.01U.385.547	Management appliance 2U 8HDD TB
DIVAR IP all-in-one 7000	DIP 7380 8HD	F.01U.385.542	Management appliance 2U 8HTLE TB
DIVAR IP all-in-one 7000	DIP 73920 00N	F.01U.385.543	Management appliance 3U without HDD
DIVAR IP all-in-one 7000	DIP 73928 16HD	F.01U.385.544	Management appliance 3U 16HDTB
DIVAR IP all-in-one 7000	DIP 73922 16HD	F.01U.385.545	Management appliance 3U 16HTLE TB

DIVAR IP all-in-one 4000

Family Name	CTN	SAP#	Material description
DIVAR IP all-in-one 4000	DIP 4422XG 00N	F.01U.404.045	Management appliance w/o HDD
DIVAR IP all-in-one 4000	DIP 4422XG 2HD	F.01U.404.047	Management appliance 2x8TB
DIVAR IP all-in-one 4000	DIP 4423XG 2HD	F.01U.404.042	Management appliance 2x8TB
DIVAR IP all-in-one 4000	DIP 4422XG 2HD	F.01U.404.043	Management appliance 2x18TB

DIVAR IP all-in-one 6000

Family Name	CTN	SAP#	Material description
DIVAR IP all-in-one 6000	DIP 6440XG 00N	F.01U.404.045	Management appliance 1U w/o HDD
DIVAR IP all-in-one 6000	DIP 6440XG 4HD	F.01U.404.046	Management appliance 1U 4x4TB

Family Name	CTN	SAP#	Material description
DIVAR IP all-in-one 6000	DIP-6466EZ-4HD	F.01U.404.047	Management appliance for BVMS
DIVAR IP all-in-one 6000	DIP-6466EZ-4HD	F.01U.404.048	Management appliance for BVMS