1 Advisory Information

- **Advisory ID:** BOSCH-SA-506619-BT
- **CVE Numbers and CVSS v3.1 Scores:**
  - CVE-2018-1285
    - Base Score: 9.8 (Critical)
- **Published:** 16 Mar 2022
- **Last Updated:** 16 Mar 2022

2 Summary

When BVMS is installed in an installation folder where low-priviledged users have write access, BVMS is affected by a security vulnerability, which potentially allows for XXE-based attacks in applications that accept attacker-controlled log4net configuration files.

Bosch rates the vulnerability with a CVSS v3.1 Base Score of 5.7 (Medium) when the BVMS is installed in default location.

Bosch recommends customers to follow the least priviledge-approach for user permissions in the BVMS installation folder.

3 Affected Products

- Bosch BVMS <= 9.0.0
- Bosch BVMS 10.0 <= 10.0.2
- Bosch BVMS 10.1 <= 10.1.1
- Bosch BVMS 11.0 <= 11.1.0
- Bosch DIVAR IP 7000 R2
- Bosch DIVAR IP all-in-one 5000
- Bosch DIVAR IP all-in-one 7000

4 Solution and Mitigations

4.1 Install BVMS into a directory where low-privileged OS users do not have write permissions

BVMS relies on its installation directory to be trustworthily protected against modification by non-administrators. When BVMS is installed in the default location %ProgramFiles%, the vulnerability can only be exploited when an attacker already possesess administrative priviliges in the OS prior to the actual attack.

Bosch strongly recommends not to install BVMS into a directory where low-privileged OS users have write permissions.

5 Vulnerability Details

5.1 CVE-2018-1285

CVE description: Apache log4net versions before 2.0.10 do not disable XML external entities when parsing log4net configuration files. This allows for XXE-based attacks in applications that accept attacker-controlled log4net configuration files.

- Problem Type:
  - CWE-611
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 9.8 (Critical)

6 Remarks

6.1 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.

6.2 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.

7 Additional Resources

- [1] Third Party Supplier Advisory: https://issues.apache.org/jira/browse/LOG4NET-575
- [2] CVE: https://nvd.nist.gov/vuln/detail/CVE-2018-1285

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

8 Revision History

- 16 Mar 2022: Initial Publication

9 Appendix

9.1 Modified CVSS Score

CVSS Base Score: 5.7 (Medium) CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:L/I:L/A:L

9.2 Affected Products

product	version	configuration
BVMS	<=11.1.0	Default BVMS installation folder requires administrative priviledges for modification.
DIVAR IP	with BVMS <=11.1.0	In default factory settings BVMS installation folder requires administrative priviledges for modification.

9.3 Material Lists

9.3.1 BVMS

Family Name	CTN	SAP#	Material description
BVMS Professional 11.1	MBV-BPRO	F.01U.393.647	License Professional base
BVMS Plus 11.1	MBV-BPLU	F.01U.393.650	License Plus base
BVMS Viewer 11.1	MBV-BVWR	F.01U.393.649	License Viewer base
BVMS Lite 11.1	MBV-BLIT	F.01U.393.648	License Lite base
BVMS Professional 11.0	MBV-BPRO	F.01U.393.647	License Professional base
BVMS Plus 11.0	MBV-BPLU	F.01U.393.650	License Plus base
BVMS Viewer 11.0	MBV-BVWR	F.01U.393.649	License Viewer base
BVMS Lite 11.0	MBV-BLIT	F.01U.393.648	License Lite base
BVMS Professional 10.1	MBV-BPRO-101	F.01U.389.492	License Professional base
BVMS Enterprise 10.1	MBV-BENT-101	F.01U.389.506	License Enterprise base
BVMS Plus 10.1	MBV-BPLU-101	F.01U.389.477	License Plus base
BVMS Viewer 10.1	MBV-BVWR-101	F.01U.389.508	License Viewer base
BVMS Lite16 10.1	MBV-BLIT-101	F.01U.389.465	License Lite base
BVMS Professional 10.0	MBV-BPRO-100	F.01U.362431	License Professional base
BVMS Enterprise 10.0	MBV-BENT-100	F.01U.362432	License Enterprise base
BVMS Plus 10.0	MBV-BPLU-100	F.01U.362445	License Plus base
BVMS Viewer 10.0	MBV-BVWR-100	F.01U.362471	License Viewer base
BVMS Lite 10.0	MBV-BLIT-100	F.01U.362455	License Lite base

9.3.2 Bosch 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 4x3TB
DIVAR IP 7000 R2	DIP-7183-8HD	F.01U.314.522	DIVAR IP 7000 2U 8x3TB
DIVAR IP 7000 R2	DIP-7184-4HD	F.01U.314.523	DIVAR IP 7000 2U 4x4TB
DIVAR IP 7000 R2	DIP-7184-8HD	F.01U.314.524	DIVAR IP 7000 2U 8x4TB
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 16x3TB
DIVAR IP 7000 R2	DIP-71F4-16HD	F.01U.314.527	DIVAR IP 7000 3U 16x4TB

Family Name	CTN	SAP#	Material description
DIVAR IP 7000 R2	DIP-7186-8HD	F.01U.329.143	DIVAR IP 7000 2U 8x6TB
DIVAR IP 7000 R2	DIP-7188-8HD	F.01U.329.144	DIVAR IP 7000 2U 8x8TB
DIVAR IP 7000 R2	DIP-71F6-16HD	F.01U.329.145	DIVAR IP 7000 3U 16x6TB
DIVAR IP 7000 R2	DIP-71F8-16HD	F.01U.329.146	DIVAR IP 7000 3U 16x8TB
DIVAR IP 7000 R2	DIP-7184-8HD-WAG	F.01U.343.277	DIVAR IP 7000 2U 8x4TB, WAG Kit

9.3.3 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
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

9.3.4 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

9.3.5 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 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