# Product Security Information
## Microsoft SQL Server
## Apache Log4j 1.x Vulnerabilities
## BOSCH-SI-2023-0801BT

### Overview

This Product Security Information affects the Apache Log4j 1.2.17 library, a widely used logging component in Java-based applications. The purpose of this information is to advise about the potential risk and to clarify its impact on a BVMS system. The vulnerable component is not actively used or called by the SQL Server or by the BVMS for which the vulnerabilities are not exploitable. If the CVE’s appear due to conducting a vulnerability scan in the BVMS, they can be dismissed as a false positive.

### Technical Details

#### 1.1 Risk Assessment

We have identified that the vulnerable Log4j 1.2.17 component is installed as part of the setup of Microsoft SQL Server 2019 on Windows, all editions. The vulnerable component is not actively used or called by the SQL Server or by the BVMS. This means that the vulnerabilities are not exploitable unless you install some additional components that refer to the vulnerable component. Therefore, there is no risk of exploitation within the SQL Server or BVMS environment.

#### 1.2 Considered Common Vulnerability and Exposure (CVE)

CVE-2019-17571 (CVSS v3 Base Score: 9.8)
CVE-2020-9488 (CVSS v3 Base Score: 3.7)
CVE-2021-4104 (CVSS v3 Base Score: 7.5)
CVE-2022-23302 (CVSS v3 Base Score: 8.8)
CVE-2022-23305 (CVSS v3 Base Score: 9.8)
CVE-2022-23307 (CVSS v3 Base Score: 8.8)
CVE-2023-26464 (CVSS v3 Base Score: 7.5)

#### 1.3 Exploitability

CVE-2019-17571
Log4j includes a SocketServer that accepts serialized log events and deserializes them without verifying whether the objects are allowed or not.

CVE-2020-9488

Improper validation of certificate with host mismatch in Apache Log4j SMTP appender. This could allow an SMTPS connection to be intercepted by a man-in-the-middle attack which could leak any log messages sent through that appender.

CVE-2021-4104
JMSAppender uses JNDI in an unprotected manner allowing any application using the JMSAppender to be vulnerable if it is configured to reference an untrusted site or if the site referenced can be accesseed by the attacker. For example, the attacker can cause remote code execution by manipulating the data in the LDAP store.

CVE-2022-23302
JMSSink uses JNDI in an unprotected manner allowing any application using the JMSSink to be vulnerable if it is configured to reference an untrusted site or if the site referenced can be accessed by the attacker. For instance, the attacker can cause remote code execution by manipulating the data in the LDAP store.

CVE-2022-23305
A SQL injection flaw in JDBCAppender that allows the data being logged to modify the behaviour of the component. By design, the JDBCAppender in Log4j 1.2.x accepts an SQL statement as a configuration parameter where the values to be inserted are converters from PatternLayout. The message converter, %m, is likely to always be included. This allows attackers to manipulate the SQL by entering crafted strings into input fields or headers of an application that are logged allowing unintended SQL queries to be executed.

CVE-2022-23307
A deserialization flaw was found in Apache Chainsaw component in Log4j 1.x., which could lead to malicious code execution.

### 1.4 References

https://logging.apache.org/log4j/1.2/

## Bosch Products

BVMS 11.0
BVMS 11.1
BVMS 11.1.1
BVMS 12.0
BVMS 12.0.1
Bosch DIVAR IP all-in-one 7000 R3
Bosch DIVAR IP 7000 R2
Bosch DIVAR IP all-in-one 5000
Bosch DIVAR IP all-in-one 7000
DIVAR IP all-in-one 4000
DIVAR IP all-in-one 6000

## Mitigations

Despite the BVMS itself not being vulnerable, we recommend that you take precautionary measures and install the latest cumulative update for SQL Server 2019 to mitigate any future risks. Microsoft has provided KB5011644 - Cumulative Update 16 for SQL Server 2019, which removes the vulnerable log4j component.

Bosch has tested Cumulative Update 21 for SQL Server 2019, which was the latest update at the time of testing, and which removed the vulnerable log4j component.

Detailed information about Cumulative Update 16 can be found here: https://learn.microsoft.com/en-us/troubleshoot/sql/releases/sqlserver-2019/cumulativeupdate16

Detailed information about the tested Cumulative Update 21 can be found here: https://learn.microsoft.com/en-us/troubleshoot/sql/releases/sqlserver-2019/cumulativeupdate21

## Material Lists

**BVMS**

| Family Name | CTN | SAP# | Material description |
|---|---|---|---|
| BVMS Professional 12.0.1 | MBV-BPRO | F.01U.393.647 | License Professional base |
| BVMS Plus 12.0.1 | MBV-BPLU | F.01U.393.650 | License Plus base |
| BVMS Plus 12.0.1 DIP | MBV-BPLU-DIP | F.01U.374.503 | License Plus base for DIVAR IP |
| BVMS Lite 12.0.1 | MBV-BLIT | F.01U.393.648 | License Lite base |
| BVMS Lite 12.0.1 DIP | MBV-BLIT-DIP | F.01U.358.975 | License Lite base for DIVAR IP |
| BVMS Professional 12.0 | MBV-BPRO | F.01U.393.647 | License Professional base |
| BVMS Plus 12.0 | MBV-BPLU | F.01U.393.650 | License Plus base |
| BVMS Plus 12.0 DIP | MBV-BPLU-DIP | F.01U.374.503 | License Plus base for DIVAR IP |
| BVMS Lite 12.0 | MBV-BLIT | F.01U.393.648 | License Lite base |
| BVMS Lite 12.0 DIP | MBV-BLIT-DIP | F.01U.358.975 | License Lite base for DIVAR IP |
| BVMS Professional 11.1.1 | MBV-BPRO | F.01U.393.647 | License Professional base |
| BVMS Plus 11.1.1 | MBV-BPLU | F.01U.393.650 | License Plus base |
| BVMS Plus 11.1.1 DIP | MBV-BPLU-DIP | F.01U.374.503 | License Plus base for DIVAR IP |
| BVMS Lite 11.1.1 | MBV-BLIT | F.01U.393.648 | License Lite base |
| BVMS Lite 11.1.1 DIP | MBV-BLIT-DIP | F.01U.358.975 | License Lite base for DIVAR IP |
| 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 Plus 11.1 DIP | MBV-BPLU-DIP | F.01U.374.503 | License Plus base for DIVAR IP |
| BVMS Lite 11.1 | MBV-BLIT | F.01U.393.648 | License Lite base |

| | | | |
|---|---|---|---|
| BVMS Lite 11.1 DIP | MBV-BLIT-DIP | F.01U.358.975 | License Lite base for DIVAR IP |
| 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 Plus 11.0 DIP | MBV-BPLU-DIP | F.01U.374.503 | License Plus base for DIVAR IP |
| BVMS Lite 11.0 | MBV-BLIT | F.01U.393.648 | License Lite base |
| BVMS Lite 11.0 DIP | MBV-BLIT-DIP | F.01U.358.975 | License Lite base for DIVAR IP |

**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 |
| 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 |

**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 |

**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 |

**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 |

**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 |

**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 |

# 5 Document Change Log

2023.08.23 – Revision 1.00: Initial Release