# Product Security Information

## Apache Log4j 1.x Vulnerabilities on MegaRAID Storage Manager (MSM)

## BOSCH-SI-2023-0802BT

### Overview

The MegaRAID Storage Manager (MSM) is a Broadcom Inc. software used to configure, monitor, and maintain MegaRAID Serial-attached SCSI (SAS) RAID controllers. MegaRAID Storage Manager (MSM) versions before 17.05.06.00 are affected by Apache Log4j v1.x vulnerabilities and therefore this information aims to clarify the impact of the Apache Log4j v1.x vulnerabilities on a Bosch DIVAR IP system and provide guidelines to upgrade the MegaRAID Storage Manager (MSM) software, which is strongly advised to fix the vulnerabilities and reinforce the security of the system.

### Affected Products

Bosch DIVAR IP 6000 R2
Bosch DIVAR IP 7000 R2
Bosch DIVAR IP all-in-one 7000 (DIP-72xx)
Bosch DIVAR IP all-in-one 7000 (DIP-73xx)

### Technical Details

#### 1.1 Considered Common Vulnerabilities and Exposures (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)

#### 1.2 Vulnerability Details

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 accessed 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.

CVE-2023-26464
When using the Chainsaw or SocketAppender components with Log4j 1.x on JRE less than 1.7, an attacker that manages to cause a logging entry involving a specially-crafted (ie, deeply nested) hashmap or hashtable (depending on which logging component is in use) to be processed could exhaust the available memory in the virtual machine and achieve Denial of Service when the object is deserialized.

### 1.3 References

https://logging.apache.org/log4j/1.2/
https://docs.broadcom.com/docs/17.05.06.00_MSM.txt

## Solution and Mitigations

The MSM 17.05.06.00 version has been released to add enhancements, fix bugs and fix the log4j v.1.2 reported vulnerabilities as per in the release notes 17.05.06.00_MSM.txt. To upgrade your DIVAR IP all-in-one unit please carry out the following actions, specified, and advised by Broadcom:

1) Before the MSM upgrade, download all required files to a USB stick:
   - Download the 32-bit/x86 JRE binary, recommended and tested JRE version: jdk8u372-b07. Notice MSM is a 32-bit application, so ensure the download of the 32-bit/x86 JRE binary.
   - Download the jdk8u372-b07 binary checksum file: OpenJDK8U-jre_x86-32_windows_hotspot_8u372b07.zip.sha256.txt
   - Download the MegaRAID Storage Manager v17.05.06.00 installation package.

2) Plug-in the USB stick on the DIVAR IP and copy the installation files. (Assume: C:\Users\Administrator\Downloads):

3) Set up the Java Runtime Environment (JRE).
   - Open the PowerShell as Administrator and validate the integrity of the JRE binary (assume: C:\Users\Administrator\Downloads):

```
# Checksum value available in the file: OpenJDK8U-jre_x86-32_windows_hotspot_8u372b07.zip.sha256.txt
Get-FileHash -Algorithm SHA256 OpenJDK8U-jre_x86-32_windows_hotspot_8u372b07.zip
```

- Unzip the OpenJRE file in your desired location (assume: C:\jre folder).

  *mkdir C:\jre*
  *Expand-Archive OpenJDK8U-jre_x86-32_windows_hotspot_8u372b07.zip -D C:\jre*
  *# On DIVAR IP 6000 R2 and 7000 R2 extract the archive manually to the directory 'C:\jre'*

- Create the JRE_HOME as a system-wide variable.

  *setx /M JRE_HOME C:\jre\jdk8u372-b07-jre*

- To validate the variable creation, close the PowerShell and open a new window still as Administrator to ensure the variable is loaded and run the command:

  *# Expected result: C:\jre\jdk8u372-b07-jre*
  *$Env:JRE_HOME*

4) Upgrade the MegaRaid Storage Manager application.
   - Unzip the zip file (assume: C:\Users\Administrator\Downloads):

     *Expand-Archive 17.05.06.00_MSM_Windows.zip*
     *# On DIVAR IP 6000 R2 and 7000 R2 extract the archive manually to the directory 'C:\Users\Administrator\Downloads\17.05.06.00_MSM_Windows'.*

   - Ensure the files have not been corrupted during download:

     *cd 17.05.06.00_MSM_Windows*
     *# MSM17050600.zip checksum is available in the MD5CheckSum.txt file*
     *Get-FileHash -Algorithm MD5 MSM17050600.zip*

   - Unzip the MSM17050600.zip file:

     *Expand-Archive MSM17050600.zip*
     *# On DIVAR IP 6000 R2 and 7000 R2 extract the archive manually to the directory 'C:\Users\Administrator\Downloads\17.05.06.00_MSM_Windows\MSM17050600'.*

   - Run the setup.exe installation file to upgrade the MSM:

     *cd .\MSM17050600\DISK1*
     *.\setup.exe /s /v"/qn UPGRADEONLY=1 SETUPTYPE=Complete"*

     *! If after the upgrade the MegaRAID Storage Manager stop working, go to "C:\Users\Administrator\Downloads\17.05.06.00_MSM_Windows\MSM17050600\DISK1", run the MegaRAID Storage Manager (MSM) setup.exe and on the InstallShield Wizard select Repair to repair installation errors in the program.*

5) The upgrade will run in the background silently up to a minute. Open the MegaRAID Storage Manager application afterward and the new version should be available.

6) A README file is available in the 17.05.06.00 MSM with detailed information about the upgrade. It can be used to support the installation process or troubleshooting.

Notice!
For consistent functionality, compatibility, performance, and security, regularly update the software to the latest version throughout the operational life of the device.

# Material Lists

## Bosch DIVAR IP 6000 R2

| Family Name | CTN | SAP# | Material description |
|---|---|---|---|
| DIVAR IP 6000 R2 | DIP-6180-00N | F.01U.308.406 | DIVAR IP 6000 2U w/o HDD |
| DIVAR IP 6000 R2 | DIP-6183-4HD | F.01U.308.452 | DIVAR IP 6000 2U 4x3TB |
| DIVAR IP 6000 R2 | DIP-6183-8HD | F.01U.308.453 | DIVAR IP 6000 2U 8x3TB |
| DIVAR IP 6000 R2 | DIP-6184-4HD | F.01U.308.454 | DIVAR IP 6000 2U 4x4TB |
| DIVAR IP 6000 R2 | DIP-6184-8HD | F.01U.308.455 | DIVAR IP 6000 2U 8x4TB |
| DIVAR IP 6000 R2 | DIP-61F0-00N | F.01U.308.456 | DIVAR IP 6000 3U w/o HDD |
| DIVAR IP 6000 R2 | DIP-61F3-16HD | F.01U.308.457 | DIVAR IP 6000 3U 16x3TB |
| DIVAR IP 6000 R2 | DIP-61F4-16HD | F.01U.308.458 | DIVAR IP 6000 3U 16x4TB |
| DIVAR IP 6000 R2 | DIP-6186-8HD | F.01U.329.139 | DIVAR IP 6000 2U 8x6TB |
| DIVAR IP 6000 R2 | DIP-6188-8HD | F.01U.329.140 | DIVAR IP 6000 2U 8x8TB |
| DIVAR IP 6000 R2 | DIP-61F6-16HD | F.01U.329.141 | DIVAR IP 6000 3U 16x6TB |
| DIVAR IP 6000 R2 | DIP-61F8-16HD | F.01U.329.142 | DIVAR IP 6000 3U 16x8TB |

## 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 7000 (DIP-72xx)

| 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 |

## Bosch DIVAR IP all-in-one 7000 (DIP-73xx)

| 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 |

## Document Change Log

2023.08.23 – Revision 1.00: Initial Release