Industrial HiVision 08.1.00 was released

2019-12-20 - Christoph Strauss - Software Products

Security Vulnerability Corrected in version 08.1.00

Vulnerability	Description
Java CVE-2019-2933	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data.
Java CVE-2019-2945	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded.
Java CVE-2019-2958	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data.
Java CVE-2019-2962	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded.

Java CVE-2019-2964	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Concurrency). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded.
Java CVE-2019-2978	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded.
Java CVE-2019-2983	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded.
Java CVE-2019-2989	Vulnerability in the Oracle GraalVM Enterprise Edition product of Oracle GraalVM (component: Java). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle GraalVM Enterprise Edition. While the vulnerability is in Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle GraalVM Enterprise Edition accessible data.
Java CVE-2019-2988	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded.
Java CVE-2019-2992	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded.
Java CVE-2019-2894	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Security). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data.

Java CVE-2019-2996	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Deployment). Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data.
Java CVE 2019-10086	In Apache Commons Beanutils 1.9.2, a special BeanIntrospector class was added which allows suppressing the ability for an attacker to access the classloader via the class property available on all Java objects. However, this is not used by the default characteristic of the PropertyUtilsBean.
Java CVE 2019-12384	FasterXML jackson-databind 2.x before 2.9.9.1 might allow attackers to have a variety of impacts by leveraging failure to block the logback-core class from polymorphic deserialization. Depending on the class-path content, remote code execution may be possible.
Java CVE 2019-14379	SubTypeValidator.java in FasterXML jackson-databind before 2.9.9.2 mishandles default typing when ehcache is used (because of net.sf.ehcache.transaction.manager.DefaultTransactionManagerLookup), leading to remote code execution.
Java CVE 2019-14439	A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.x before 2.9.9.2. This occurs when Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has the logback jar in the classpath.
Java CVE 2019-14540	A Polymorphic Typing issue was discovered in FasterXML jackson-databind before 2.9.10. It is related to com.zaxxer.hikari.HikariConfig.
Java CVE 2019-16335	A Polymorphic Typing issue was discovered in FasterXML jackson-databind before 2.9.10. It is related to com.zaxxer.hikari.HikariDataSource. This is a different vulnerability than CVE-2019-14540.

Issues fixed in version 08.1.00

- You can find the problems, workarounds and fixes related to this release in the issue list.

New features in version 08.1.00

- New features:
  - You can protect the Edit Mode, when an edit mode password is assigned or the user management is active.
  - Password change for the first time login on a device
  - Forward events to a syslog server over TLS
  - Configurable auto-acknowledge function, when the status changes for an event
  - Generate test events when configuring status configuration
  - Globally Enable/Disable monitoring of the Security Status
  - Start HiProvision from Industrial HiVision
  - Show number of selected list entries
  - When configuring event actions, you can test the action during the configuration.
  - Certificates are stored in a key store for sub-domain interfaces.
  - The user can now reset the icon on multiple devices to the default icon, as long as there are only devices selected.
-
- New devices:
  - Hi-SCOM BN48 and BN3049
- MultiConfig™ dialogs added:
  - Switching - MRP-IEEE - MVRP Configuration (HiOS)
  - Switching - GARP - GMRP (HiOS)
  - Switching - GARP - GVRP (HiOS)
  - Switching - VLANs - Voice (Classic Software, HiOS)
  - Routing - ARP - Global (Classic Software)
  - Diagnostics - Email Notification - Global - Create Email Subject (HiOS)
  - Diagnostics - Ports - Port-Mirroring (HiOS)
  - Port Dialog: Port - Port Security (Classic Software, HiOS)
  - Port Dialog: Port - Dynamic ARP Inspection (HiOS)
  - Port Dialog: Port - MRP-IEEE - Configuration (HiOS)
  - Port Dialog: Port - MRP-IEEE - MMRP (HiOS)
  - Port Dialog: Port - MRP-IEEE - MVRP (HiOS)
  - Port Dialog: Port - GARP - GMRP (HiOS)
  - Port Dialog: Port - GARP - GVRP (HiOS)
  - Port Dialog: Port - DHCP L2 Relay (HiOS)
  - Port Dialog: Port - DHCP Server (HiOS)
  - Port Dialog: Port - Profinet IO (HiOS)

-
- MultiConfig™ dialogs modified:
    - Routing - ARP - Global (HiOS, HiSecOS)
    - Diagnostics - Email Notification - Global (HiOS)
    - Diagnostics - Email Notification - Mail Server (HiOS)
    - Port Dialog: Port - POE (Classic Software, HiOS)
-

Additions to the manual in version 08.1.00

- The following sentence, "Industrial HiVision enters DeviceConfig_<IP-Adresse>, is changed to "Industrial HiVision enters <IP-Address> in the File Name field".
- In chapter "8.2.24 Properties of a component detail", section "Generate test events" (page 301):
  Ignore item 8 of the "Generate test events procedure":
  'In the "Import event" dialog, verify that the table displays the event for which you wish to assign an action'.

This version has been tested with the following firmware versions:

Device	Firmware version
BAT54RAIL	8.80
BAT54RAIL-PLUS	8.80
BAT-R	9.12
BAT-F	9.12
BAT-C	2.3.8

Device	Firmware version
BAT-2C	08.02.01.02
BAT450-F	9.12
BAT867-R	9.12
Bobcat	07.4.01
Dragon PTN	2.4.52
Dragon MACH4000	07.4.00
Dragon MACH4500	7.2.02
DX940-2GSFP-4TX-4RS-T1-H	4.0.0
DX1000-TS-02-H	3.1.8
EAGLE Ruggedized	HiSecOS-01.1.01
EAGLE Ruggedized	HiSecOS-01.2.00
EAGLE Ruggedized	HiSecOS-03.0.00
EAGLEONE-TX-TX	ONE-05.3.00
EAGLE20-TX-TX	SDV-05.3.02
EES25-0600	HiOS-2E-04.0.00
EESX20-0800	HiOS-2E-04.0.00
EESX30-0600	HiOS-2E-06.0.00
Gecko 4TX	01.0.01
GRS1020-8T8Z	HiOS-2S-06.0.00
GRS1020-16T9	HiOS-2S-04.1.00
HiProvision	V04.0.14
IS30	V011R021
LioN-R	V1.0.10.8-1.4
MACH 3001	3.46
MACH 3002	3.46
MACH100	L2P-09.0.12

Device	Firmware version
MACH1000GE	L3P-08.0.08
MACH4000 48G	L3P-08.0.08
MACH4002-24G	L2P-09.0.08
MACH4002-24G-3X	L3P-09.0.04
Magnum 10RX	4.0.4C1
MAR1030	L2P-09.0.11
MAR1040	L2P-09.0.12
MAR1040	L3P-09.0.12
MS20-0800	L2P-08.0.04
MS20-2400	L2E-09.0.07
MS2108-2	4.06
MS30-0802	L2E-09.0.07
MS4128-5	L3P-09.0.07
MSP30-2404	HiOS-2A-07.0.00
OCTOPUS 3	HiOS-07.5.00
OCTOPUS-8M	L2P-09.0.07
OS30-001604	HiOS-2S-04.1.02
PowerMICE	L3P-08.0.08
RED25-04002T1TT	HiOS-2S-PRP-06.0.00
RS20-0400	L2E-09.0.12
RS20-0800M2	L2E-09.0.12
RS20-1600M2	L2E-09.0.12
RS20-2500M3	L2P-09.0.12
RS2-16M	9.07
RS2-TX-TX	9.07
RS30-0802	L2P-09.0.12

Device	Firmware version
RS30-2402	L2P-09.0.12
RS40-0009	L2P-09.0.12
RSB20	L2B-05.3.05
RSP25-11003Z6ZT	HiOS-2S-PRP-06.0.00
RSP35-08033O6TT	HiOS-2S-06.0.00
RSPE32-24044O7T99	HiOS-3S-04.0.00
RSR20-08TP	L2P-09.0.12
RSR30-06TP-03COMBO	L2P-09.0.12

Gerelateerde inhoud

- HAC_Issue-List_2019-12-19.pdf
- ihivision08100_linux.tar.download.zip
- ihivision08100_windows.exe.download.zip