Industrial HiVision 08.0.02 was released

2020-04-03 - Christoph Strauss - Software Products

Security Vulnerability Corrected in version 08.0.02

Vulnerability	Description
Java CVE-2020-2583	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions that are affected are Java SE and Java SE Embedded. 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-2020-2590	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Security). Supported versions that are affected are Java SE and Java SE Embedded. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Kerberos to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data.
Java CVE-2020-2593	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported versions that are affected are Java SE and Java SE Embedded. 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 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-2020-2601	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Security). Supported versions that are affected are Java SE and Java SE Embedded. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Kerberos to compromise Java SE, Java SE Embedded. While the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded accessible data.
Java CVE-2020-2604	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions that are affected are Java SE and Java SE Embedded. 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 takeover of Java SE, Java SE Embedded.
Java CVE-2020-2654	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected is Java SE. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE.
Java CVE-2020-2659	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported versions that are affected are Java SE and Java SE Embedded. 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-2020-8840	FasterXML jackson-databind 2.0.0 through 2.9.10.2 lacks certain xbean-reflect/JNDI blocking, as demonstrated by org.apache.xbean.propertyeditor.JndiConverter.
Java CVE-2020-9546	FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to org.apache.hadoop.shaded.com.zaxxer.hikari.HikariConfig (aka shaded hikari-config).
Java CVE-2020-9547	FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to com.ibatis.sqlmap.engine.transaction.jta.JtaTransactionConfig (aka ibatis-sqlmap).
Java CVE-2020-9548	FasterXML jackson-databind 2.x before 2.9.10.4 mishandles the interaction between serialization gadgets and typing, related to br.com.anteros.dbcp.AnterosDBCPConfig (aka anteros-core).
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-2019-2933	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-2019-2988	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-2019-2989	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-2019-2992	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-2019-2996	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.
Java CVE-2019-20330	FasterXML jackson-databind 2.x before 2.9.10.2 lacks certain net.sf.ehcache blocking.

New features in version 08.0.02

- Edit Mode password protection when the user management is active

Issues fixed in version 08.0.02

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

Related Content

- HAC_Issue-List_2020-03-31.pdf
- ihivision08002_linux.tar.download.zip
- ihivision08002_windows.exe.download.zip