HiFusion v04.1.00 was released

2019-12-20 - - Software Products

Security Vulnerability Corrected in version 04.1.00

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 04.1.00

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

Conteúdo relacionado

- HAC_Issue-List_2019-12-18.pdf

- hifusion04100_linux.tar.download.zip
- hifusion04100_windows.exe.download.zip