Sense of Security	Authorisation. Jason Edelstein
	Release date. 19 July 2011.

Sense of Security – Security Advisory – SOS-11-009.

Oracle Sun GlassFish Enterprise Server Stored XSS Vulnerability.

19 July 2011.

GlassFish Enterprise Server Stored XSS - Security Advisory - SOS-11-009

Release Date.	19-Jul-2011
Last Update.	-
Vendor Notification Date.	23-Mar-2011
Product.	Sun GlassFish Enterprise Server
Platform.	Java EE
Affected versions.	2.1.1 ((v2.1 Patch06)(9.1_02 Patch12))(build b31g-fcs) verified, possibly others
Severity Rating.	Medium
Impact.	Cookie/credential theft, impersonation, loss of confidentiality
Attack Vector.	Remote without authentication
Solution Status.	Vendor patch
CVE reference.	CVE-2011-2260
Oracle Bug ID.	7030596

Details.

GlassFish is an open source application server project led by Sun Microsystems for the Java EE platform. The proprietary version is called Sun GlassFish Enterprise Server. GlassFish supports all Java EE API specifications, such as JDBC, RMI, e-mail, JMS, web services, XML, etc, and defines how to coordinate them.

Stored:

The log viewer fails to securely output encode logged values. As a result, an unauthenticated attacker can trigger the application to log a malicious string by entering the values into the username field. This will cause the application to log the incorrect login attempt and results in a stored XSS vulnerability. When an administrator logs into the application and views the log, the malicious code will be executed in the client browser. As an example, navigate to:

http://[host]:4848

Enter the below into the login field:

'>"><script>alert(3);</script>

When the user views the “Search Log Files” page, the above client-side code will be executed in the client browser. The offending script is

http://[host]:4848/logViewer/logViewer.jsf

Reflected:

By modifying the windowTitle or helpFile variables of /com_sun_webui_jsf/help/helpwindow.jsf it is possible to trigger a reflected XSS vulnerability. An example is shown below:

/com_sun_webui_jsf/help/helpwindow.jsf?&windowTitle=Help+Window'>"><script>alert(1);</script>&helpFile=commontask.html

/com_sun_webui_jsf/help/helpwindow.jsf?&windowTitle=Help+Window&helpFile=commontask.html'>"><script>alert(1);</script>

Solution.

Apply the vendor patch.

Discovered by.

Sense of Security Labs.

About us.

Sense of Security is a leading provider of information security and risk management solutions. Our team has expert skills in assessment and assurance, strategy and architecture, and deployment through to ongoing management. We are Australia’s premier application penetration testing firm and trusted IT security advisor to many of the country’s largest organisations.

Sense of Security Pty Ltd

Level 8, 66 King St
Sydney NSW 2000
AUSTRALIA

T: +61 (0)2 9290 4444
F: +61 (0)2 9290 4455
W: http://www.senseofsecurity.com.au
E: info@senseofsecurity.com.au
Twitter: @ITsecurityAU

The latest version of this advisory can be found at:

http://www.senseofsecurity.com.au/advisories/SOS-11-009.pdf

Other Sense of Security advisories can be found at:

http://www.senseofsecurity.com.au/research/it-security-advisories.php