	Authorisation. Jason Edelstein
	Release date. 05 September 2012.

Sense of Security – Security Advisory – SOS-12-009.

Ektron CMS - Multiple Vulnerabilities.

05 September 2012.

Sense of Security	Authorisation. Jason Edelstein
	Release date. 05 September 2012.

Ektron CMS – Multiple Vulnerabilities - Security Advisory - SOS-12-009

Release Date.	05-Sep-2012
Last Update.	-
Vendor Notification Date.	07-May-2012
Product.	Ektron CMS
Platform.	ASP.NET
Affected versions.	Ektron CMS version 8.5.0 and possibly others
Severity Rating.	High
Impact.	Exposure of sensitive information Exposure of system information System access
Attack Vector.	Remote without authentication
Solution Status.	Fixed in version 8.6 (not verified by SOS)
CVE reference.	CVE- not yet assigned

Details.

The web application is vulnerable to multiple security vulnerabilities, such as unauthenticated file upload and XML eXternal Entities (XXE) injection.

1. Unauthenticated File Upload:

The form /WorkArea/Upload.aspx does not require authentication to upload a file. By issuing a POST request with a webshell embedded in a JPEG image and specifying the ASPX extension it is possible to upload ASPX code to /uploadedimages/. The ASPX code is placed in the comment section of the JPEG so that it survives image resizing.

2. XXE Injection:

The XML parser at /WorkArea/Blogs/xmlrpc.aspx is vulnerable to XML external entity attacks which can be used to scan behind perimeter firewalls or possibly include files from the local file system e.g.

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

<scan>&amp;amp;test;</scan>
```

Solution.

Upgrade to version 8.6 and remove the /WorkArea/Blogs/xmlrpc.aspx file.

Discovered by.

Phil Taylor and 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.

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/consulting/penetration-testing
E: info@senseofsecurity.com.au
Twitter: @ITsecurityAU

The latest version of this advisory can be found at:

http://www.senseofsecurity.com.au/advisories/SOS-12-009.pdf

	Authorisation. Jason Edelstein
	Release date. 05 September 2012.

Other Sense of Security advisories can be found at:

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