Sense of Security – Security Advisory – SOS-12-008.

Elcom CMS - Community Manger Insecure File Upload Vulnerability.

24 August 2012.

Elcom CMS – Community Manager Insecure File Upload - Security Advisory - SOS-12-008

Release Date.	24-Aug-2012
Last Update.	-
Vendor Notification Date.	28-Oct-2011
Product.	Elcom CMS – Community Manager
Platform.	ASP.NET
Affected versions.	Elcom Community Manager version 7.4.10 and possibly others
Severity Rating.	High
Impact.	Exposure of sensitive information Exposure of system information System access
Attack Vector.	Remote with authentication (publisher privilege)
Solution Status.	Fixed in version 7.5 and later (not verified by SOS)
CVE reference.	CVE- not yet assigned

Details.

The https://[server]/UploadStyleSheet.aspx script does not validate the file type passed in the parameter “myfile0” on the server side allowing the uploading and execution of ASPX files. An attacker can upload an ASPX web shell and execute commands with web server user privileges.

Proof of Concept.

A shell uploaded using the vulnerable (https://[server]/UploadStyleSheet.aspx) script can be accessed at the following location:
https://[server]/UserUploadedStyles/shell.aspx

Solution.

Upgrade to version 7.5 or later.

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-12-008.pdf

Other Sense of Security advisories can be found at:

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