Sense of Security	Authorisation. Jason Edelstein
	Release date. 20th December 2010.

Sense of Security – Security Advisory – SOS-10-004.

Elcom Technology's CommunityManager.NET Auth Bypass Vulnerability.

20th December 2010.

CommunityManager.NET Auth Bypass - Security Advisory - SOS-10-004

Release Date.	20-Dec-2010
Last Update.	-
Vendor Notification Date.	22-Jan-2010
Product.	Elcom Technology's CommunityManager.NET
Platform.	IIS with ASP.NET
Affected versions.	CommunityManager.NET v6.7 verified and possibly others
Severity Rating.	High
Impact.	Application "System" user access
Attack Vector.	Remote without authentication
Solution Status.	Vendor patch
CVE reference.	Not yet assigned

Details.

The web application uses cookie parameters passed via HTTP requests to identify which user is logged in. Authentication routines can be bypassed by simply appending the below POC string to a cookie which already contains a valid ASP.NET session ID. The value given to the various cookie parameters indicates the specific user ID for the application user the attacker wishes to impersonate.

Proof of Concept.

To exploit this vulnerability, simply browse to the software to automatically create a valid ASP.NET session ID. Once obtained, add the following to the cookie parameter:

; CMLogUserwww2=21; OnlineLearnUserwww2=21

Note that the ID value of "21" in the above instance indicates that the user with the user ID of "21" will be impersonated. If this user ID is not linked to a user account,

access will not be obtained. Some enumeration or educated guessing may be required.

Solution.

Sense of Security has been advised that Elcom Technology has patched all versions of CommunityManager.NET and notified all clients.

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 countries 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-10-004.pdf

Other Sense of Security advisories can be found at:

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